A TREATISE

ON

THE THEORY

OF

ALGEBRAICAL EQUATIONS.

BY

J. HYMERS, D.D.

LATE FELLOW AND TUTOR OF ST JOHN'S COLLEGE, CAMBRIDGE.

THIRD EDITION ENLARGED

Cambridge:

DEIGHTON, BELL AND CO.

LONDON:

WHITTAKER AND CO. AND BELL AND DALDY.

1858.

Cambridge:
PRINTED BY C. J. CLAY, M.A.
AT THE UNIVERSITY PRESS

CONTENTS.

SECTION I.

ON THE GENERAL PROPERTIES OF EQUATIONS.

SECTION II.

ON THE TRANSFORMATION OF EQUATIONS.

..ION III.

.. THE ROOTS OF EQUATIONS.

SECTION IV.

ON THE DEPRESSION OF EQUATIONS, SOME OF WHOSE ROOTS HAVE PARTICULAR RELATIONS TO ONE ANOTHER; OR ARE OF A PARTICULAR FORM.

SECTION V.

OF THE GENERAL SOLUTION OF EQUATIONS OF A DEGREE INFERIOR TO THE FIFTH.

SECTION VI.

ON THE SEPARATION OF THE ROOTS OF EQUATIONS.

SECTION VII.

ON THE METHODS OF FINDING APPROXIMATE VALUES OF THE REAL INCOMMENSURABLE ROOTS OF EQUATIONS.

SECTION VIII.

ON SYMMETRICAL FUNCTIONS OF THE ROOTS OF EQUATIONS.

SECTION IX.

ON ELIMINATION.

SECTION X.

ON THE GENERAL SOLUTION OF EQUATIONS OF ALL DEGREES.

SECTION XI.

ON SOME PROPERTIES OF NUMBERS.

Students reading this Work for the first time may confine their attention to the following Articles:

1—21; 23—34; 36—42; 46—48; 50—52; 55—57; 59, 60; 64—66; 69, 70; 72, 74—77; 82—88; 93, 94, 122; 128—138; 143, 144; 148—151; 168—170. Afterwards they may add Art. 22, Exs. 1—15; 35, 44, 49, 54, 67, 89. 100—104, 123, 126, 127, 140, 154, 158, 160, 161, 165, 172.



THEORY OF EQUATIONS.

SECTION I.

ON THE GENERAL PROPERTIES OF EQUATIONS.

DEFINITIONS AND PRINCIPLES.

1. EVERY equation under a rational form involving the powers of only one unknown quantity x, may, by dividing its two members by the coefficient of the highest power of x, and transposing the terms, be reduced to the form

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n = 0;$$

where x^n, the highest power of x, is positive, and its coefficient is unity; and p_1, p_2, ... p_n, the coefficients of the other powers of x, are known quantities which may be positive, or negative, or zero.

The equation is said to be of the number of dimensions, or of the degree, which is expressed by the index of the highest power of x which it involves; and to be complete, when it contains all the other inferior powers of x, and a constant or absolute term; otherwise, to be incomplete.

Every quantity or expression, real or imaginary, which, when substituted for x in the expression $x^n + p_1 x^{n-1} + \ldots + p_n$, makes the whole vanish, is called a root of the equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n = 0.$$

To solve an equation is to find all its roots.

OBS. To effect the general solution of equations, would be to find the expressions for all the roots of an equation of

any assigned degree in terms of its coefficients, the coefficients being general symbols. This has hitherto been done only for equations of a degree not exceeding the 4^{th}; and even for cubic equations, it will be seen that the functions of the coefficients which express the roots, are insufficient to give the numerical values of the roots when they are all real; hence we are led to suppose that if we could obtain general formulæ for the roots of equations of the 5^{th} and superior degrees, we should be unable to obtain from them the numerical values of the roots by the simple substitution of the numerical values of the coefficients.

This supposition has been confirmed by the successive investigations of Geometers, who have shewn that the general solution of an equation whose coefficients are indeterminate, and whose roots have no particular relations to one another, is impossible beyond the fourth degree. It has also been shewn by Abel that, if two roots are so connected that one of them can be expressed rationally in terms of the other, the equation, if its degree be a prime number, is solvable by radicals; and if a composite number, its solution depends on that of equations of inferior degrees. And more recently Gallois has demonstrated that, in order that an irreducible equation, whose degree is a prime number, may be solvable by radicals, it is necessary and sufficient that, any two of its roots being given, the others can be obtained rationally from them.

2. It has therefore become necessary to invent methods for obtaining, either exactly or approximately, the roots of numerical equations; and which, although only applicable to such equations, depend for their demonstration upon certain general properties of equations. The investigations constituting the Theory of Equations, which may in general be conducted by processes purely algebraical and elementary, besides affording a knowledge which will have its use in almost every branch of Analysis, will be found particularly serviceable as an exercise to the mathematical student; they

naturally distribute themselves under these three heads, 1st those relating to the general theory of equations, that is, to the properties which are common to all equations; 2ndly, to the solution of numerical equations, that is, to the determination of values either exact or approximate of the roots of an equation whose coefficients are given numbers; and 3rdly, to the algebraical solution of equations, that is, to the determination of an expression composed of the coefficients of a given equation, which, substituted for the unknown quantity, shall identically satisfy the equation. These investigations it is the object of the following Treatise to exhibit; not under the separate heads above named, but intermixed in such a manner as shall seem most convenient to the learner.

3. If the signs of the terms of any equation be all positive, it cannot have a positive root; and if the signs of a complete equation be alternately positive and negative, it cannot have a negative root.

For, in the former case, every positive quantity, substituted for x, will give a positive result, instead of making the whole vanish, and therefore cannot be a root; and in the latter case, every negative quantity, substituted for x, will give a positive or negative result, according as the degree of the equation is even or odd, instead of making the whole vanish, and therefore cannot be a root.

4. If a quantity a be a root of the equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0,$$

the first member is divisible by $x - a$ without a remainder, and conversely.

Suppose the expression $x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n$, which we shall hereafter denote by $f(x)$, to be divided by $x - a$; now since $x - a$ is only of one dimension with respect to x, the division may be carried on till we obtain a remainder independent of x; let Q be the quotient, in which only positive powers of x will enter, and R the remainder;

$$\therefore f(x) = Q \, . \, (x - a) + R \; \ldots\ldots \; (1).$$

In this identical equation write a for x, then the first member becomes zero, because a is a root of $f(x)=0$; also the term $Q.(x-a)$ vanishes, since one of its factors vanishes and the other cannot become infinite; therefore $R=0$; and since R does not contain x, it is not altered by substituting a for x, and therefore zero is the value of R in equation (1), whatever be the value of x; that is, $f(x)$ is exactly divisible by $x-a$.

Conversely, if the expression $x^n+p_1x^{n-1}+\ldots+p_n$ be divisible by $x-a$ without a remainder, a is a root of the equation

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots+p_n=0.$$

For, $f(x)=Q.(x-a)$, where Q is a polynomial containing only positive powers of x; if therefore $x=a$, $f(a)=0$, or a is a root of the equation $f(x)=0$.

5. Hence, since a is evidently a root of $x^n-a^n=0$, x^n-a^n is divisible by $x-a$, whether n be odd or even;

and the quotient $=x^{n-1}+ax^{n-2}+a^2x^{n-3}+\ldots+a^{n-1}$.

Also, when n is even, x^n-a^n is divisible by $x+a$; since in that case, $-a$ is a root of $x^n-a^n=0$.

When n is odd, $-a$ is a root of $x^n+a^n=0$; therefore in this case, x^n+a^n is divisible by $x+a$, but not by $x-a$. If n is even, x^n+a^n is divisible by neither $x+a$ nor $x-a$.

6. To find the quotient and remainder, when the expression $x^n+p_1x^{n-1}+\ldots+p_n$ is divided by $x-a$, a being any quantity.

Let the division be carried on till the remainder is independent of x, and let Q be the quotient and R the remainder;

$$\therefore\ x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots+p_n=Q(x-a)+R\ldots\ldots(1),$$

in which identical equation, since R does not contain x, and Q contains only positive powers of x, if we write a for x, we get

$$a^n+p_1a^{n-1}+p_2a^{n-2}+\ldots+p_n=R;$$

that is, the remainder, after dividing $f(x)$ by $x-a$, is equal to $f(a)$, the value assumed by $f(x)$ when in it a is written for x.

Next, substituting this value of R in equation (1) and transposing, we have

$$x^n - a^n + p_1(x^{n-1} - a^{n-1}) + p_2(x^{n-2} - a^{n-2}) + \dots$$
$$+ p_{n-1}(x-a) = Q(x-a);$$

but the quantities $x^n - a^n$, $x^{n-1} - a^{n-1}$, ... are all divisible by $x - a$; therefore, effecting the division, we get (Art. 5)

$$x^{n-1} + ax^{n-2} + a^2x^{n-3} + \dots + a^{n-1}$$
$$+ p_1(x^{n-2} + ax^{n-3} + a^2x^{n-4} + \dots + a^{n-2}) + \dots + p_{n-1} = Q;$$

or, arranging the result according to powers of x,

$$Q = x^{n-1} + (a+p_1)\,x^{n-2} + (a^2 + p_1a + p_2)\,x^{n-3} +$$
$$(a^3 + p_1a^2 + p_2a + p_3)\,x^{n-4} + \dots + (a^{n-1} + p_1a^{n-2}$$
$$+ p_2a^{n-3} + \dots + p_{n-1});$$

that is, in the quotient of $f(x)$ divided by $x-a$, the coefficient of the first term x^{n-1} is unity; and the coefficients of the other terms are formed, one from the other, by multiplying the coefficient of the preceding term by a, and adding the coefficient of that term in $f(x)$, which involves the same power of x as the preceding term does.

EXISTENCE OF ROOTS AND FACTORS.

7. If two quantities a and b, when substituted for x in the expression $f(x)$, give results affected with different signs, one root at least of the equation $f(x) = 0$ lies between them.

Suppose $a < b$, and suppose a to give a positive result, and b a negative result, when substituted for x in the expression $f(x)$. Let P be the sum of the positive, N the sum of the negative terms in $f(x)$; then when $x = a$, $P - N$ is positive or $P > N$, and when $x = b$, $P - N$ is negative or $P < N$; let x change by insensible degrees from a to b, then P and N both increase, but P increases slower than N, since when

$x=b$, $P<N$; consequently, for some intermediate value of x between a and b, $P=N$, or $P-N=0$, or $f(x)$ becomes equal to zero; this value therefore is a root of the equation.

If the smaller quantity a gave a negative result, the proof would be precisely similar.

Also, since the first member of the equation may pass several times from positive to negative, or from negative to positive, by the substitution of gradually ascending values between a and b, it follows that several roots of $f(x)=0$ may be comprised between a and b, and we are certain that one is.

8. Hence, if there exist no real quantity which, substituted for x, will make $f(x)$ vanish, $f(x)$ must be positive for every value of x; for if $f(x)$ became negative for any value b, since by putting it under the form

$$f(x)=x^n\left(1+\frac{p_1}{x}+\frac{p_2}{x^2}+\dots+\frac{p_n}{x_n}\right),$$

and substituting ∞, that is a quantity indefinitely large, for x, we necessarily obtain a positive result $(\infty)^n$ (the quantity within the brackets being reduced to unity), the equation $f(x)=0$ would have a real root, lying between b and ∞ (Art. 7), which is contrary to the supposition.

Also, if in $f(x)$, we substitute $-\infty$ for x, we evidently get a result $(-\infty)^n$; i. e. $+\infty$, or $-\infty$, according as n is even or odd.

9. It is always possible to assign such a finite positive value to x, that for that and every greater value, $f(x)$ shall be positive; and such a finite negative value, that for that and every greater negative value, $f(x)$ shall be positive or negative, according as n is even or odd.

Let p be the greatest coefficient without regard to signs; then if

$$x^n>p\,(x^{n-1}+x^{n-2}+\dots+x+1)>p\,\frac{x^n-1}{x-1},$$

we shall of course have

$$x^n>p_1x^{n-1}+p_2x^{n-2}+\dots+p_{n-1}x+p_n;$$

because in the latter inequality some of the terms may be negative, and no positive term is greater than the corresponding term in the former case. Now the inequality

$$x^n > p\,\frac{x^n - 1}{x - 1} \text{ is satisfied, if } x^n = \text{or} > x^n\,\frac{p}{x-1},$$

or if $x =$ or $> p + 1$; therefore $p + 1$, and every greater number, is a value of x which makes the first term of $x^n + p_1 x^{n-1} + \ldots + p_n$ greater than the sum of all the other terms; or makes the value of $f(x)$ positive.

Again, let $x = -y$; then, according as n is even or odd,

$$x^n + p_1 x^{n-1} + \ldots + p_{n-1} x + p_n \text{ becomes}$$
$$y^n - p_1 y^{n-1} + \ldots - p_{n-1} y + p_n,$$
$$\text{or } -(y^n - p_1 y^{n-1} + \ldots + p_{n-1} y - p_n).$$

Now by what has already been proved, the value $p + 1$, and every greater value for y, makes the former expression positive, and the latter negative; but this value of y corresponds to $-(p + 1)$ for x, at the same time that the preceding functions of y correspond to $f(x)$; therefore the value $-(p+1)$, or any greater negative value for x, makes $x^n + p_1 x^{n-1} + \ldots + p_n$ positive or negative, according as n is even or odd.

This proposition shews what term in $f(x)$ is the most important, when very large values are given to x; viz. the term which involves the highest power of x; since a moderate value $p + 1$ for x makes x^n exceed the aggregate of the remaining terms of $f(x)$.

10. Every equation of an odd degree has at least one real finite root of a sign contrary to that of its last term; and every equation of an even degree with its last term negative has at least two real finite roots of different signs.

First, let the equation be of an odd degree with its last term negative; then $x = 0$ gives a negative result, and $x = p + 1$ gives a positive result (p being the greatest coefficient without regard to signs); therefore the equation has at least

one real positive root between 0 and $p+1$. If the last term be positive, then $x=0$ gives a positive result, and $x=-(p+1)$ gives a negative result; therefore the equation has at least one real negative root between 0 and $-(p+1)$.

Secondly, let the equation be of an even degree with its last term negative; then $x=0$ gives a negative result, and each of the values, $x=p+1$, $x=-(p+1)$, gives a positive result; therefore the equation has at least two real roots, one positive between 0 and $p+1$, and the other negative between 0 and $-(p+1)$.

OBS. The mere existence of the roots may be proved, without reference to Art. 9, as follows.

In an equation of an odd degree, if the last term be negative, $x=0$ gives a negative result, and $x=\infty$ gives a positive result; therefore, there is at least one real root between 0 and ∞, or one positive root. Similarly, if the last term be positive, $x=0$, $x=-\infty$, gives results with different signs, and therefore include between them at least one real negative root.

If the equation be of an even degree with its last term negative, then $x=0$ gives a negative result, and $x=\pm\infty$, a positive result; therefore the equation has at least two real roots of different signs.

11. If an equation have only one change of signs, it can only have one positive root.

Since the equation has only one change of signs, it will have one or more positive terms, and all the rest will be negative; therefore (Art. 10) it will necessarily have a positive root a; let $p_r x^{n-r}$ be the last positive term, and let the equation be divided by x^{n-r}, and it will be

$$x^r + p_1 x^{r-1} + \dots + p_r - \left(\frac{p_{r+1}}{x} + \dots + \frac{p_n}{x^{n-r}}\right) = 0\,;$$

then when $x=a$, the two parts become equal, but if $x>a$, the first part increases and the second diminishes; and if

$x < a$ (continuing positive), the first part diminishes and the second increases; therefore it is impossible that for any positive value except $x = a$, the two parts should be equal, or that the equation should have more than one positive root.

12. Hence, we are certain of the existence of a real finite root in every equation unless it be of an even degree with its last term positive, in which case it may have no real root; but then there may, and, as will hereafter be shewn, must exist an impossible expression of the form $\alpha + \beta\sqrt{-1}$ (α and β being possible quantities) which, substituted for x in $f(x)$, will make the whole vanish. We shall therefore, for the present, assume that every equation admits a root of the form $\alpha + \beta\sqrt{-1}$, α and β being real finite quantities, or either of them being zero; that is, we shall assume, not only that every equation has a root expressible by algebraical symbols, but that $\alpha + \beta\sqrt{-1}$ is the form which the root necessarily takes.

13. Every equation has as many roots as it has dimensions, and no more.

Since every equation has necessarily a root real or imaginary, let a_1 be a root of $f(x) = 0$; then $f(x)$ is divisible by $x - a_1$; let $f_1(x)$ be the quotient,

$$\therefore f(x) = (x - a_1) f_1(x),$$

$f_1(x)$ denoting a polynomial of $n - 1$ dimensions, exactly similar* to $f(x)$, and having therefore the same properties. Hence $f_1(x) = 0$ must have a root real or imaginary; let this be a_2, and let $f_2(x)$, a polynomial of $n - 2$ dimensions, be the quotient of $f_1(x)$ divided by $x - a_2$;

$$\therefore f_1(x) = (x - a_2) f_2(x),$$

$$\text{and } f(x) = (x - a_1)(x - a_2) f_2(x).$$

Similarly, $f_2(x) = (x - a_3) f_3(x)$; and proceeding in this manner, we shall at last come to a quotient of only one dimension in x, $(x - a_n) f_n(x)$, where $f_n(x)$ is numerical, and

must equal unity, because the coefficient of x^n in $f(x)$ is unity, so that

$$f_{n-2}(x) = (x - a_{n-1}) f_{n-1}(x) = (x - a_{n-1})(x - a_n);$$

therefore, by successive substitutions, we have

$$f(x) = (x - a_1)(x - a_2)(x - a_3) \dots (x - a_{n-1})(x - a_n).$$

Now in order that the product of n simple factors may vanish, it is sufficient that any one of the factors should vanish; therefore we shall satisfy the equation $f(x) = 0$, by giving to x any one of the n values $a_1, a_2, a_3, \dots a_n$.

Neither can we satisfy it by any other values; for, if possible, let e be a root of $f(x) = 0$, e being different from each of the quantities $a_1, a_2, \dots a_n$; then $f(e)$ or $(e - a_1)(e - a_2) \dots (e - a_n)$ must be equal to zero; but this is impossible since not one of the factors is so; therefore e is not a root. Therefore every equation of the n^{th} degree has n roots, and no more; and every polynomial of the n^{th} degree is resolvable into one determinate system of n simple factors.

Obs. In the above proposition, the divisors are not necessarily different from one another; any number, or all, of them may be alike: and it is in this sense that an equation is said to have as many roots as it has dimensions, namely, that its first member is resolvable into as many simple factors, equal or unequal, as it has dimensions, each of which equated to zero will furnish a root; so that as many times as any factor $x - a$ occurs in its first member, so many roots equal to a will the equation have. As the existence of equal roots in an equation can be easily detected, and the equation cleared of them, we shall in general suppose that to be the case; in order to get rid of exceptions to which several of our conclusions would otherwise be liable.

14. If a polynomial of the n^{th} order,

$$f(x) = p_0 x^n + p_1 x^{n-1} + p_2 x^{n-2} + \&c. + p_{n-1} x + p_n,$$

be made identically equal to zero by more than n different values of x, then each coefficient p_0, p_1, &c. must be separately

equal to zero, and $f(x)$ must be identically equal to zero for every value of x; for, otherwise, the equation $f(x)=0$, would be satisfied by more than n different values of x, which is impossible.

Hence, also, if we have, for more than n different values of x,

$$p_0x^n+p_1x^{n-1}+\&c.+p_n=p'_0x^n+p'_1x^{n-1}+\&c.+p'_n,$$

since this equation may be written

$$(p_0-p'_0)\,x^n+(p_1-p'_1)\,x^{n-1}+\&c.+p_n-p'_n=0,$$

we must have $p_0=p'_0$, $p_1=p'_1$, &c., $p_n=p'_n$; and the two polynomials will be identical for every value of x.

15. Hence, if we know a root a of the equation $f(x)=0$, we may divide the first member by $x-a$, and the quotient put equal to zero, will be an equation, one dimension lower, containing the remaining roots; or we may form the reduced equation immediately, without the trouble of division, by the rule of Art. 6. Similarly, if we know two roots a and b of $f(x)=0$, by dividing its first member by $(x-a)\,(x-b)$, and putting the quotient equal to zero, we shall obtain an equation, two dimensions lower, containing the remaining roots. And in general, if we know $n-r$ roots of $f(x)=0$, by dividing $f(x)$ by the product of the simple factors corresponding to these roots, we may form the reduced equation of r dimensions, $\phi(x)=0$, containing the remaining roots; and if $f(x)=0$ has only $n-r$ real roots, then all the roots of $\phi(x)=0$ are imaginary, and in this case $\phi(x)$ is a polynomial of an even number of dimensions with its last term positive, and is incapable of being made negative by any real value of x, (Arts. 8 and 12).

Hence also, if all the real roots $a_1, a_2, \dots a_{n-r}$, of an equation of n dimensions have been obtained, the equation will be

$$(x-a_1)\,(x-a_2)\dots(x-a_{n-r})\,.\,\phi(x)=0,$$

where $\phi(x)$ is such as has been described.

16. **Impossible roots enter equations by pairs, each pair corresponding to a real quadratic factor of the polynomial forming the first member.**

Let $\alpha+\beta\sqrt{-1}$ represent one of the imaginary roots, and let it be substituted for x in the first member of the equation $f(x)=0$. The result will consist of two parts, possible quantities which involve the powers of α and the even powers of $\beta\sqrt{-1}$, and impossible quantities which involve the odd powers of $\beta\sqrt{-1}$; let P be the sum of the possible quantities, and $Q\beta\sqrt{-1}$ that of the impossible quantities; therefore the whole result is

$$P+Q\beta.\sqrt{-1},$$

where P and Q contain only even powers of β.

Now since $\alpha+\beta\sqrt{-1}$ is a root,

$$P+Q\beta\sqrt{-1}=0;$$

and as no part of P can be destroyed by $Q\beta\sqrt{-1}$, this resolves itself into $P=0$, $Q=0$. Now for x substitute $\alpha-\beta\sqrt{-1}$, or change the sign of β in the former result; then since P and Q contain only even powers of β, the result is

$$P-Q\beta\sqrt{-1},$$

which, since $P=0$, $Q=0$, is equal to zero; therefore $\alpha-\beta\sqrt{-1}$ is a root of $f(x)=0$. Therefore the proposed equation admits a pair of roots $\alpha+\beta\sqrt{-1}$ and $\alpha-\beta\sqrt{-1}$, which are said to be conjugate to one another; and its first member admits the two factors

$$x-\alpha-\beta\sqrt{-1},\quad x-\alpha+\beta\sqrt{-1},$$

and will therefore be divisible by their product which equals

$$(x-\alpha)^2+\beta^2 \text{ or } x^2-2\alpha x+\alpha^2+\beta^2.$$

In the same manner it might be shewn that when the coefficients are rational, surd-roots of the form $a\pm\sqrt{b}$ enter equations by pairs.

17. Hence the total number of impossible roots in any equation will always be even; and every equation of an even degree may be resolved into real factors of the second degree; for every pair of impossible roots will produce a real quadratic factor; and the possible roots, since there is an even number of them, may also be divided into pairs, each of which will produce a real factor of the second degree.

Also, since $f(x)$, a polynomial of the n^{th} degree, always admits n divisors real or imaginary of the first degree, it will admit $\frac{n(n-1)}{1.2}$ different divisors, real or imaginary, of the second degree; $\frac{n(n-1)(n-2)}{1.2.3}$ of the third degree; &c.; and, in general, it will admit $\frac{n(n-1)\ldots(n-r+1)}{1.2.3\ldots r}$ of the r^{th} degree, as each of these will be a combination of r out of the n simple factors. Also the total number of divisors of all degrees will be $2^n - 1$.

18. To actually decompose the first member of a given equation $f(x) = 0$, into its real, simple or quadratic factors, is the great problem to the solution of which all enquiries in this subject are directed; but the inverse problem, to form the equation when the roots are given, offers no difficulty; for, knowing the component factors of the polynomial forming its first member, we can determine that polynomial by the common process of multiplication. Thus, to form the equation whose roots are $a, -b, c, c, \alpha \pm \beta\sqrt{-1}$, we must multiply together the factors

$$x - a,\ x + b,\ (x - c)^2,\ x^2 - 2\alpha x + \alpha^2 + \beta^2.$$

RELATIONS BETWEEN THE COEFFICIENTS AND ROOTS.

19. To find the relations between the coefficients and roots of an equation.

We must first ascertain the law of formation of the products of any number of binomial factors $x + a$, $x + b$, $x + c$,

&c., which have all the same first term x, but different second terms a, b, c, &c.

By actual multiplication we get

$$(x+a)(x+b) = x^2 + (a+b)x + ab$$

$$(x+a)(x+b)(x+c) = x^3 + (a+b+c)x^2 + (ab+ac+bc)x + abc$$

$$(x+a)(x+b)(x+c)(x+d) = x^4 + (a+b+c+d)x^3 + (ab+ac+ad+bc+bd+cd)x^2 + (abc+abd+acd+bcd)x + abcd.$$

In these products we observe that the index of x diminishes by unity in each term, from the first term where it is the same as the number of factors, to the last where it is zero; also the coefficient of the first term is unity, that of the second is the sum of the second terms of the binomial factors, that of the third term is the sum of the products of every two, that of the fourth term is the sum of the products of every three, and the last term is the product of all the second terms of the binomial factors. To prove these laws of the indices and coefficients generally true, we must shew that if they be true for $n-1$ factors, they will be true for n factors. Let therefore the product of $n-1$ factors

$$(x+a)(x+b)(x+c)\dots(x+k) = x^{n-1} + S_1x^{n-2} + S_2x^{n-3} + \dots + S_{r-1}x^{n-r} + \dots + S_{n-1},$$

where S_1, S_2, &c. denote the sum, the sum of the products of every two, &c., of the $n-1$ quantities $a, b, c \dots k$. Now introduce another factor $x+l$, and we find for result

$$x^n + (S_1+l)x^{n-1} + (S_2+lS_1)x^{n-2} + \dots + (S_r+lS_{r-1})x^{n-r} + \dots + lS_{n-1}.$$

With respect to the indices, the law is unchanged; with respect to the coefficients, that of the first term is still unity; that of the 2nd

$$= S_1 + l = \text{sum of the } n \text{ quantities } a, b, c, \dots l;$$

that of the 3rd

$= S_2 + lS_1 =$ sum of the products of every two;

that of the $(r+1)^{th}$

$= S_r + lS_{r-1} =$ sum of the products of every r;

and the last term

$= lS_{n-1} =$ the product of the n quantities.

If therefore the law of formation of the product be true for $n-1$ factors, it is true for n; but it is verified for 2, 3, &c., factors, therefore it is generally true.

Now let $a, b, c, \dots l$ be the n roots of the equation $f(x)=0$; then

$$x^n + p_1 x^{n-1} + \dots + p_r x^{n-r} + \dots + p_n$$
$$= (x-a)(x-b)(x-c)\dots(x-l)$$
$$= x^n + S_1 x^{n-1} + S_2 x^{n-2} + \dots + S_r x^{n-r} + \dots + S_n,$$

where S_1, S_2, &c. denote the sums of the various combinations (taken singly, two and two, &c.) of $-a$, $-b$, &c.; that is, of the roots with their signs changed; therefore, equating coefficients,

$$p_1 = S_1,\ p_2 = S_2, \dots p_r = S_r,\ p_n = S_n;$$

or, coefficient of 2nd term with its proper sign = sum of the roots with their signs changed;

coefficient of 3rd term with its proper sign = sum of the products of every two roots with their signs changed;

coefficient of the $(r+1)^{th}$ term with its proper sign = sum of the products of every r roots with their signs changed;

and the last term with its proper sign = the product of all the roots with their signs changed.

Or, if we choose, which is more convenient, to employ in the ennunciation both the roots and the coefficients with their proper signs, we have

$-p_1 =$ sum of the roots,

$p_2 =$ sum of the products of every two,

$-p_3 =$ sum of the products of every three;

and generally,

$(-1)^r p_r =$ sum of the products of every r roots.

20. These relations, which furnish n equations between the roots and the coefficients, do not afford any immediate means of finding the roots; and if we wished to employ them to find one of the roots by the elimination of the $n-1$ others, we should always arrive at an equation similar to the proposed.

Let, for example, the equation be of the third degree,

$$x^3+p_1x^2+p_2x+p_3=0, \text{ roots } a, b, c;$$

$$\therefore p_1=-(a+b+c),$$

$$p_2=ab+ac+bc,$$

$$p_3=-abc;$$

to eliminate b and c between these three equations, multiply the first by a^2, and the second by a, and add them to the third, and we find

$$a^3+p_1a^2+p_2a+p_3=0.$$

21. But although not leading to the determination of the roots, the above relations will enable us to discover many of their properties; and they are to be regarded as constituting one of the fundamental propositions of the Theory of Equations. At present we shall employ them to find the values of some of the more common symmetrical functions of the roots; that is, of functions in which each root is alike involved, so that their values are unaltered when any two of the roots are interchanged.

(1) To find the sum of the squares of the roots of $f(x)=0$.

$$-p_1=a+b+c+\ldots+l;$$

$$\therefore p_1^2=a^2+b^2+c^2+\ldots+l^2+2(ab+ac+bc+\ldots)$$

$$=\text{sum of squares}+2p_2;$$

$$\therefore \text{sum of squares}=p_1^2-2p_2.$$

(2) To find the sum of the reciprocals of the roots.

$$(-1)^{n-1}p_{n-1}=bc\ldots l+ac\ldots l+ab\ldots l+\ldots$$

$$(-1)^n p_n=abc\ldots l;$$

$$\therefore \frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\ldots+\frac{1}{l}=-\frac{p_{n-1}}{p_n}.$$

(3) To find the sum of $\frac{a}{b}+\frac{b}{a}+\frac{a}{c}+\frac{c}{a}+\ldots$

$$\text{This} = a\left(\frac{1}{a}+\frac{1}{b}+\ldots+\frac{1}{l}\right)-1+b\left(\frac{1}{a}+\frac{1}{b}+\ldots+\frac{1}{l}\right)-1+\ldots$$

$$=(a+b+\ldots+l)\left(\frac{1}{a}+\frac{1}{b}+\ldots+\frac{1}{l}\right)-n$$

$$=(-p_1)\left(-\frac{p_{n-1}}{p_n}\right)-n=\frac{p_1p_{n-1}}{p_n}-n.$$

---

22. The following are examples of depressing an equation when one or more of its roots are known; or of forming it when all its roots are known; also of resolving certain polynomials into their factors.

(1) To find the roots of $x^3-1=0$.

One root is $x=1$; dividing by $x-1$, we get the quadratic $x^2+x+1=0$ containing the other two roots, and which gives for their values

$$x=\frac{-1\pm\sqrt{-3}}{2}.$$

(2) To find the roots of $x^5-9x^3+x^2-9=0$.

The first member $=x^3(x^2-9)+x^2-9=(x^3+1)(x^2-9)$

$$=(x+1)(x^2-x+1)(x+3)(x-3);$$

therefore the five values of x are

$$-1,\ -3,\ 3,\ \frac{1\pm\sqrt{-3}}{2}.$$

(3) A root of

$$x^9+x^8-9x^7+3x^6-8x^5+8x^4-3x^3+9x^2-x-1=0$$

is unity; it is required to form the equation containing the remaining roots; it is (Art. 6)

$$x^8+(1+1)x^7+(2-9)x^6+(-7+3)x^5+(-4-8)x^4$$
$$+(-12+8)x^3+(-4-3)x^2+(-7+9)x+(2-1)=0;$$
$$\text{or } x^8+2x^7-7x^6-4x^5-12x^4-4x^3-7x^2+2x+1=0.$$

(4) To form the equation whose roots are

$$4,\ -1,\ \tfrac{1}{2}(-3\pm\sqrt{-31}).$$

It is $(x-4)(x+1)(x^2+3x+10)=0$;

$$\text{or } x^4-3x^2-42x-40=0.$$

Similarly, the biquadratic with real coefficients, one of whose roots is $\frac{1}{2}(\sqrt{3}+\sqrt{-1})$, is $x^4-x^2+1=0$.

(5) The equation of eight dimensions (in which the coefficients are dependent upon one another by particular relations)

$$x^8+4nx^6+2x^4-4nx^2+1=0,$$

may be solved as a quadratic; for it becomes successively

$$\left(x^2+\frac{1}{x^2}\right)^2+4n\left(x^2-\frac{1}{x^2}\right)=0,$$

$$\left(x^2-\frac{1}{x^2}\right)^2+4n\left(x^2-\frac{1}{x^2}\right)+4n^2=4(n^2-1),$$

$$x^2-\frac{1}{x^2}=2\sqrt{n^2-1}-2n,\quad x^4-2x^2(\sqrt{n^2-1}-n)=1;$$

and by reason of the double values of the radical quantities involved, the eight roots are expressed by one formula

$$x=\sqrt{(\sqrt{n+1}-\sqrt{n})(\sqrt{n-1}+\sqrt{n})}.$$

SOLUTION OF BINOMIAL EQUATIONS WITH THE HELP OF A TABLE OF SINES.

(6) The preceding is an instance of what must happen whenever the general solution of any equation can be effected, as stated in Art. 2. We shall next give an example of an

equation of the n^{th} degree, where it is possible to get a formula expressing the n roots and no other quantities, viz. the binomial equation

$$x^n \pm 1 = 0.$$

This is almost the only extensive class of equations that has been solved by a general method; and the discussion of the nature and properties of the roots is of great interest and importance in the Theory of Equations. It is convenient to consider the two cases $x^n - 1 = 0$ and $x^n + 1 = 0$ separately.

(7) All the roots of $x^n - 1 = 0$ are impossible, except one when n is odd, and two when n is even.

If we expel the factors $x - 1$ or $x^2 - 1$ according as n is odd or even, the depressed equations are

$$x^{n-1} + x^{n-2} + \ldots + x + 1 = 0,$$

$$x^{n-2} + x^{n-4} + \ldots + x^2 + 1 = 0;$$

of which, the former cannot have a positive root, and it cannot have a negative root since the proposed cannot have a negative root, n being odd; and the latter, since it contains only even powers of x, can neither have a positive nor a negative root; therefore the depressed equations have all their roots impossible.

Since the proposed equation is the same as $x^n = 1$, the condition which it expresses is, that the arithmetical or algebraical values of x are such, that, being raised to the n^{th} power, they produce unity. On this account the roots of $x^n - 1 = 0$ are called the n^{th} roots of unity.

(8) To solve the equation $x^n - 1 = 0$.

Since the equation can only have the real roots 1 and -1, we may assume $x = \cos\theta \pm \sqrt{-1} \sin\theta$; for this value will coincide with the real roots when θ is zero or a multiple of π, and in all other cases will be imaginary. Then *De Moivre's* formula gives

$$x^n = \cos n\theta \pm \sqrt{-1} \sin n\theta;$$

therefore all values of θ determined by the condition

$$\cos n\theta \pm \sqrt{-1} \sin n\theta = 1,$$

will give values of x which are roots of the proposed; therefore we must separately have

$$\sin n\theta = 0, \quad \cos n\theta = +1,$$

and consequently $n\theta$ must be an even multiple of π, $= 2\lambda\pi$ suppose, where λ is any integer whatever. Hence all values of x comprised in the formula

$$x = \cos \frac{2\lambda\pi}{n} \pm \sqrt{-1} \sin \frac{2\lambda\pi}{n} \quad \text{.........} (1)$$

are roots of $x^n - 1 = 0$, or are n^{th} roots of unity.

Moreover, this expression has n different values and no more.

For, taking λ from zero to $\frac{1}{2}(n-1)$ or $\frac{1}{2}n$ according as n is odd or even, we find in the first case, one real value $+1$ when $\lambda = 0$, and $\frac{1}{2}(n-1)$ pairs of imaginary values corresponding to values of λ from 1 to $\frac{1}{2}(n-1)$, or n values on the whole; and in the second case, we find one real value $+1$ when $\lambda = 0$, one real value -1 when $\lambda = \frac{1}{2}n$, and $\frac{1}{2}n - 1$ pairs of imaginary values corresponding to values of λ from 1 to $\frac{1}{2}n - 1$, or n values on the whole.

And all these imaginary values are different from one another, because the series of angles involved in them,

$$\frac{2\pi}{n}, \frac{4\pi}{n}, \frac{6\pi}{n}, \ldots \frac{(n-1)\pi}{n} \text{ or } \frac{(n-2)\pi}{n} \quad \text{.........} (2)$$

are all different from one another, and all less than π.

Also the formula (1) has no more than n values.

For if we take λ negative, the two values are not altered but only interchanged; and if we take $\lambda =$ or $> n$, the effect is to add a multiple of 2π to one of the angles (2) which alters neither the cosine nor sine; and lastly, if we consider the

values of x corresponding to values of λ, m and $n-m$ equally distant from 0 and n, we shall find them the same; for, taking $\lambda = n - m$,

$$x = \cos\frac{2(n-m)\pi}{n} \pm \sqrt{-1}\,\sin\frac{2(n-m)\pi}{n}$$

$$= \cos\frac{-2m\pi}{n} \pm \sqrt{-1}\,\sin\frac{-2m\pi}{n} = \cos\frac{2m\pi}{n} \mp \sqrt{-1}\,\sin\frac{2m\pi}{n},$$

the same as when $\lambda = m$; so that we can get no new values by taking λ greater than $\frac{1}{2}n$.

Therefore the formula can never assume any other values than the n different ones resulting from taking λ from 0 to $\frac{1}{2}(n-1)$ or $\frac{1}{2}n$, according as n is odd or even; since therefore the formula

$$x = \cos\frac{2\lambda\pi}{n} \pm \sqrt{-1}\,\sin\frac{2\lambda\pi}{n}$$

equally expresses all the roots of $x^n - 1 = 0$, and no other quantities, it is the complete solution of that equation.

(9) Hence we observe that for any value of λ, except zero, or $\frac{1}{2}n$ when n is even, the two corresponding roots are conjugate, and one is the reciprocal of the other; for

$$\left(\cos\frac{2\lambda\pi}{n} + \sqrt{-1}\,\sin\frac{2\lambda\pi}{n}\right)\left(\cos\frac{2\lambda\pi}{n} - \sqrt{-1}\,\sin\frac{2\lambda\pi}{n}\right) = 1.$$

Also, since

$$\cos\frac{2\lambda\pi}{n} \pm \sqrt{-1}\,\sin\frac{2\lambda\pi}{n} = \left(\cos\frac{2\pi}{n} + \sqrt{-1}\,\sin\frac{2\pi}{n}\right)^{\pm\lambda},$$

we observe the remarkable relation among the imaginary roots, that they are all powers of the first imaginary root corresponding to $\lambda = 1$, viz. $\cos\frac{2\pi}{n} + \sqrt{-1}\,\sin\frac{2\pi}{n}$; so that if we denote this by α, the series of imaginary roots will be

$$\alpha,\ \alpha^2,\ \alpha^3 \ldots \alpha^{\frac{n-1}{2}} \text{ or } \alpha^{\frac{n-2}{2}},$$

$$\frac{1}{\alpha},\ \frac{1}{\alpha^2},\ \frac{1}{\alpha^3} \ldots \frac{1}{\alpha^{\frac{n-1}{2}}} \text{ or } \frac{1}{\alpha^{\frac{n-2}{2}}};$$

or, since $\alpha^n = 1$, the lower line may be replaced by

$$\alpha^{n-1},\ \alpha^{n-2} \ldots \alpha^{\frac{n+1}{2}} \text{ or } \alpha^{\frac{n+2}{2}};$$

therefore, since $\alpha^{\frac{n}{2}} = -1$ when n is even, all the roots of $x^n - 1 = 0$ are contained in the series

$$1,\ \alpha,\ \alpha^2, \ldots \alpha^{n-2},\ \alpha^{n-1}.$$

(10) We next come to the case of $x^n + 1 = 0$, all whose roots are impossible, except one when n is odd. For if n be even, it is manifest that every real quantity, positive or negative, when substituted for x gives a positive result, and therefore cannot be a root; and when n is odd, expelling the factor $x + 1$, the depressed equation is

$$x^{n-1} - x^{n-2} + x^{n-3} - \ldots - x + 1 = 0,$$

which cannot have a negative root (Art. 3), and it cannot have a positive root because the proposed cannot have a positive root, therefore all its roots are imaginary.

(11) To solve the equation $x^n + 1 = 0$.

As before, we may assume

$$x = \cos\theta \pm \sqrt{-1}\,\sin\theta,$$

$$\therefore\ x^n = \cos n\theta \pm \sqrt{-1}\,\sin n\theta;$$

hence all values of θ which satisfy the condition

$$\cos n\theta \pm \sqrt{-1}\,\sin n\theta = -1,$$

will give values of x which are roots of the proposed; hence we must separately have $\sin n\theta = 0$, $\cos n\theta = -1$; therefore $n\theta$ must be an odd multiple of π, $= (2\lambda + 1)\,\pi$ suppose, where λ is any integer whatever. Hence all values of x comprised in the formula

$$x = \cos\frac{(2\lambda+1)\pi}{n} \pm \sqrt{-1}\,\sin\frac{(2\lambda+1)\pi}{n}$$

are roots of $x^n + 1 = 0$, or are n^{th} roots of negative unity.

Moreover, this formula will give for x, n different values and no more.

For, taking λ from 0 to $\frac{1}{2}(n-1)$ or $\frac{1}{2}n-1$, according as n is odd or even, we find, in the former case, $\frac{1}{2}(n-1)$ pairs of imaginary values corresponding to values of λ from 0 to $\frac{1}{2}(n-1)-1$, and one real value -1 for $\lambda = \frac{1}{2}(n-1)$, or n values on the whole; and, in the latter case, we find $\frac{1}{2}n$ pairs of imaginary values corresponding to values of λ from 0 to $\frac{1}{2}n-1$, or n values on the whole. And all these imaginary roots are different, because the angles involved in them

$$\frac{\pi}{n},\ \frac{3\pi}{n},\ \frac{5\pi}{n}\ldots\frac{(n-2)\pi}{n}\ \text{or}\ \frac{(n-1)\pi}{n}\ \ldots\ldots\ldots\ldots (3)$$

are all different, and less than π. And the above-mentioned n values are all which the formula can give for x. For if we take negative multiples of π, the values of x are the same as if those multiples were positive; and if we take $\lambda =$ or $> n$, the effect is to add a multiple of 2π to one of the angles (3), which alters neither the cosine nor sine. If $\lambda = n-1$,

$$x = \cos\frac{(2n-1)\pi}{n} \pm \sqrt{-1}\,\sin\frac{(2n-1)\pi}{n}$$

$$= \cos\frac{-\pi}{n} \pm \sqrt{-1}\,\sin\frac{-\pi}{n} = \cos\frac{\pi}{n} \mp \sqrt{-1}\,\sin\frac{\pi}{n},$$

the same as when $\lambda = 0$;

and if $\lambda = n-1-m$,

$$x = \cos\frac{(2n-2m-1)\pi}{n} \pm \sqrt{-1}\,\sin\frac{(2n-2m-1)\pi}{n}$$

$$= \cos\frac{(2m+1)\pi}{n} \mp \sqrt{-1}\,\sin\frac{(2m+1)\pi}{n},$$

the same as when $\lambda = m$; so that values of λ, equally distant from 0 and $n-1$, give the same values of x, and therefore we can get no new values by taking $\lambda > \frac{1}{2}(n-1)$.

Therefore the formula can never assume any other values than the n different ones resulting from taking λ from 0 to $\frac{1}{2}(n-1)$ or $\frac{1}{2}n-1$, according as n is odd or even; since therefore the formula

$$x = \cos\frac{(2\lambda+1)\pi}{n} \pm \sqrt{-1}\sin\frac{(2\lambda+1)\pi}{n},$$

equally expresses all the roots of $x^n+1=0$, and no other quantities, it is the complete solution of that equation.

(12) As in the former case, it may be shewn that if α denote the first imaginary root $\cos\frac{\pi}{n} + \sqrt{-1}\sin\frac{\pi}{n}$, all the imaginary roots may be represented by

$$\alpha,\ \alpha^3,\ \alpha^5, \ldots \alpha^{n-2} \text{ or } \alpha^{n-1},$$

$$\frac{1}{\alpha},\ \frac{1}{\alpha^3},\ \frac{1}{\alpha^5}, \ldots \frac{1}{\alpha^{n-2}} \text{ or } \frac{1}{\alpha^{n-1}};$$

or, since $\alpha^n = -1$, and therefore $\alpha^{2n} = 1$, the lower line may be replaced by

$$\alpha^{2n-1},\ \alpha^{2n-3} \ldots \alpha^{n+2} \text{ or } \alpha^{n+1};$$

therefore, since $\alpha^n = -1$ when n is odd, all the roots of $x^n+1=0$ are contained in the series

$$\alpha,\ \alpha^3, \ldots \alpha^{2n-3},\ \alpha^{2n-1}.$$

It may be observed that the case of $x^n+1=0$ (n odd), might have been reduced to that of $y^n-1=0$, by making $x=-y$.

We shall now give the resolution of $x^n \pm 1$ into its factors.

(13) To resolve x^n-1 into its factors.

Put $x^n - 1 = 0$;

$\therefore\ x^n = 1 = \cos 2\lambda\pi \pm \sqrt{-1} \sin 2\lambda\pi$, λ being any integer;

$$\therefore\ x = \cos\frac{2\lambda\pi}{n} \pm \sqrt{-1}\sin\frac{2\lambda\pi}{n},$$

a pair of values (except when $2\lambda = 0$ or any multiple of n, when there will be only one value) to which corresponds the quadratic factor

$$x^2 - 2x\cos\frac{2\lambda\pi}{n} + 1,$$

where λ begins from 1.

First, let n be even, then $+1$ and -1 are roots, and $x^2 - 1$ a factor; and, by taking λ from 1 to $\frac{1}{2}n - 1$, we obtain the other quadratic factors,

$$\therefore\ x^n - 1 = (x^2 - 1)\left(x^2 - 2x\cos\frac{2\pi}{n} + 1\right)\left(x^2 - 2x\cos\frac{4\pi}{n} + 1\right)\ldots$$

$$\ldots\left\{x^2 - 2x\cos\frac{(n-2)\pi}{n} + 1\right\}.$$

If we take λ greater than $\frac{1}{2}n - 1$, or less than 1, the factors recur.

Secondly, let n be odd, then $+1$ is a root, and $x - 1$ a simple factor; and by taking λ from 1 to $\frac{1}{2}(n-1)$, we obtain all the quadratic factors,

$$\therefore\ x^n - 1 = (x - 1)\left(x^2 - 2x\cos\frac{2\pi}{n} + 1\right)\left(x^2 - 2x\cos\frac{4\pi}{n} + 1\right)\ldots$$

$$\ldots\left\{x^2 - 2x\cos\frac{(n-1)\pi}{n} + 1\right\}.$$

(14) To resolve $x^n + 1$ into its factors.

Let $x^n + 1 = 0$;

$$\therefore\ x^n = -1 = \cos(2\lambda + 1)\pi \pm \sqrt{-1}\sin(2\lambda + 1)\pi,$$

λ being any integer;

$$\therefore\ x = \cos\frac{(2\lambda+1)\pi}{n} \pm \sqrt{-1}\sin\frac{(2\lambda+1)\pi}{n},$$

a pair of values (except when $2\lambda+1$ is any multiple of n, when there will be only one value) to which corresponds the quadratic factor

$$x^2 - 2x\cos\frac{(2\lambda+1)\pi}{n} + 1,$$

where λ begins from zero.

First, let n be even, then taking λ from 0 to $\frac{1}{2}n-1$, we have all the quadratic factors,

$$\therefore\ x^n + 1 = (x^2 - 2x\cos\frac{\pi}{n} + 1)(x^2 - 2x\cos\frac{3\pi}{n} + 1)\ldots$$

$$\ldots\{x^2 - 2x\cos\frac{(n-1)\pi}{n} + 1\}.$$

Secondly, let n be odd, then -1 is a root, and $x+1$ a simple factor; and by taking λ from 0 to $\frac{1}{2}(n-1)-1$, we find the $\frac{1}{2}(n-1)$ quadratic factors,

$$\therefore\ x^n + 1 = (x+1)(x^2 - 2x\cos\frac{\pi}{n} + 1)(x^2 - 2x\cos\frac{3\pi}{n} + 1)\ldots$$

$$\ldots\{x^2 - 2x\cos\frac{(n-2)\pi}{n} + 1\}.$$

We shall next give the resolution into its factors of another remarkable expression, which includes the preceding as particular cases; and deduce from it several important results.

(15) To resolve $x^{2n} - 2\cos\theta x^n + 1$ into its quadratic factors.

Solving the equation

$$x^{2n} - 2\cos\theta x^n + 1 = 0, \ldots\ldots\ldots\ldots\ldots (1)$$

we find

$$x^n = \cos\theta \pm \sqrt{-1}\sin\theta = \cos(2\lambda\pi+\theta) \pm \sqrt{-1}\sin(2\lambda\pi+\theta),$$

λ being any integer;

$$\therefore\ x = \cos\frac{2\lambda\pi+\theta}{n} \pm \sqrt{-1}\sin\frac{2\lambda\pi+\theta}{n}, \ldots\ldots (2)$$

a formula which gives the $2n$ values of x, and no other quan-

tities. First, taking λ from 0 to $n-1$, we obtain $2n$ different values; for if two of them were alike, for instance when $\lambda = p$, $\lambda = q$, as two angles cannot have their sines and cosines identical unless they differ by a multiple of 2π, it would be necessary that $\frac{2\pi(p-q)}{n}$ should be a multiple of 2π, which is impossible, since p and q are both less than n.

Again, suppose $\lambda = np + r$, where p is any positive or negative integer, and r is a positive integer less than n, so that λ falls beyond the limits 0 and $n-1$, and may represent any number whatever; then

$$x = \cos\left(2p\pi + \frac{2r\pi + \theta}{n}\right) \pm \sqrt{-1}\sin\left(2p\pi + \frac{2r\pi + \theta}{n}\right)$$

$$= \cos\frac{2r\pi + \theta}{n} \pm \sqrt{-1}\sin\frac{2r\pi + \theta}{n},$$

the same as when $\lambda = r$. Hence the formula can never acquire any other values than the $2n$ different ones which result from taking λ from 0 to $n-1$; it is therefore the complete solution of equation (1).

To the pair of values (2), corresponds the quadratic factor

$$x^2 - 2x\cos\frac{2\lambda\pi + \theta}{n} + 1;$$

and by taking λ from 0 to $n-1$, we shall obtain the n quadratic factors required;

$$\therefore\ x^{2n} - 2\cos\theta x^n + 1 = (x^2 - 2x\cos\frac{\theta}{n} + 1)\times$$

$$(x^2 - 2x\cos\frac{2\pi + \theta}{n} + 1)\,(x^2 - 2x\cos\frac{4\pi + \theta}{n} + 1)\ldots$$

$$\ldots\{x^2 - 2x\cos\frac{2(n-1)\pi + \theta}{n} + 1\}.$$

OBS. When n is even, since

$$\cos\frac{2\lambda\pi+\theta}{n}=-\cos\left(\frac{2\lambda\pi+\theta}{n}+\pi\right)=-\cos\left\{\frac{2(\lambda+\frac{1}{2}n)\pi+\theta}{n}\right\},$$

it appears that the factors corresponding to λ and to $\lambda+\frac{1}{2}n$ will only differ in the sign of the second term; therefore, when we have obtained the first half of the factors by taking λ from 0 to $\frac{1}{2}n-1$, we may find the next half corresponding to values of λ from $\frac{1}{2}n$ to $n-1$, by changing the signs of the second terms of the former.

(16) Also, since $x^{2n}-2\cos\theta x^n+1$ remains unaltered when we change the sign of θ, its quadratic factors may be arranged in pairs under the general form

$$x^2-2x\cos\frac{2\lambda\pi\pm\theta}{n}+1,$$

where λ is to be taken from 0 to $\frac{1}{2}n$ or $\frac{1}{2}(n-1)$ according as n is even or odd; it being observed that each of the values $\lambda=0$, $\lambda=\frac{1}{2}n$, gives only a single factor, and not a pair.

(17) To resolve $\sin n\theta$, $\cos n\theta$, into their factors, n being any integer.

We know that these can be expressed by polynomials containing only powers of $\sin\theta$, and of which in certain cases $\cos\theta$ is also a factor; our object is to determine the factors of those polynomials.

First, suppose n odd; then, both signs being taken,

$$x^{2n}-2\cos\theta x^n+1=(x^2-2x\cos\frac{\theta}{n}+1)\times$$

$$(x^2-2x\cos\frac{2\pi\pm\theta}{n}+1)(x^2-2x\cos\frac{4\pi\pm\theta}{n}+1)\ldots$$

$$\ldots\{x^2-2x\cos\frac{(n-1)\pi\pm\theta}{n}+1\}.$$

Now make $x=1$, and for $\frac{\theta}{n}$ write 2θ, and for $\frac{\pi}{n}$, 2α; and extract the square root of both sides;

$$\therefore \sin n\theta = 2^{n-1} \sin\theta \sin(2\alpha \pm \theta) \sin(4\alpha \pm \theta) \ldots$$
$$\ldots \sin\{(n-1)\alpha \pm \theta\};$$

and changing $n\theta$ into $\frac{\pi}{2} + n\theta$; that is, θ into $\theta + \alpha$, we get

$$\cos n\theta = 2^{n-1} \sin(\alpha+\theta) \sin(\alpha-\theta) \sin(3\alpha+\theta) \sin(3\alpha-\theta) \ldots$$
$$\ldots \sin\{(n-2)\alpha - \theta\} \sin(n\alpha + \theta),$$

or, since $n\alpha = \frac{\pi}{2}$,

$$\cos n\theta = 2^{n-1} \cos\theta \sin(\alpha \pm \theta) \sin(3\alpha \pm \theta) \ldots \sin\{(n-2)\alpha \pm \theta\}.$$

Now transform each pair of sines by the formula

$$\sin(\beta+\theta) \times \sin(\beta-\theta) = \sin^2\beta - \sin^2\theta,$$

and we have the required resolutions of $\sin n\theta$ and $\cos n\theta$ into their factors (n being odd),

$$\sin n\theta = 2^{n-1} \sin\theta (\sin^2 2\alpha - \sin^2\theta)(\sin^2 4\alpha - \sin^2\theta) \ldots$$
$$\ldots \{\sin^2(n-1)\alpha - \sin^2\theta\}$$

$$\cos n\theta = 2^{n-1} \cos\theta (\sin^2\alpha - \sin^2\theta)(\sin^2 3\alpha - \sin^2\theta) \ldots$$
$$\ldots \{\sin^2(n-2)\alpha - \sin^2\theta\}.$$

Similarly, when n is even, we find.

$$\sin n\theta = 2^{n-1} \cos\theta \sin\theta (\sin^2 2\alpha - \sin^2\theta)(\sin^2 4\alpha - \sin^2\theta) \ldots$$
$$\ldots \{\sin^2(n-2)\alpha - \sin^2\theta\}$$

$$\cos n\theta = 2^{n-1} (\sin^2\alpha - \sin^2\theta)(\sin^2 3\alpha - \sin^2\theta) \ldots$$
$$\ldots \{\sin^2(n-1)\alpha - \sin^2\theta\}.$$

(18) Hence we can resolve $\sin\theta$ and $\cos\theta$ into their factors.

If we change θ into $\frac{\theta}{n}$, we have, n being odd,

$$\sin\theta = 2^{n-1} \sin\frac{\theta}{n} \left(\sin^2 2\alpha - \sin^2\frac{\theta}{n}\right)\left(\sin^2 4\alpha - \sin^2\frac{\theta}{n}\right) \ldots;$$

therefore, making $\theta = 0$, since in that case $\dfrac{\sin\theta}{\sin\frac{\theta}{n}} = n$, we get

$$n = 2^{n-1}\sin^2 2\alpha \sin^2 4\alpha \ldots;$$

$$\therefore \sin\theta = n\sin\frac{\theta}{n}\left(1 - \frac{\sin^2\frac{\theta}{n}}{\sin^2 2\alpha}\right)\left(1 - \frac{\sin^2\frac{\theta}{n}}{\sin^2 4\alpha}\right)\ldots$$

Now make $n = \infty$, and observe that $\alpha = \dfrac{\pi}{2n}$, and therefore that

$$\frac{\sin\frac{\theta}{n}}{\sin 2\alpha} = \frac{\sin\frac{\theta}{n}}{\sin\frac{\pi}{n}} = \frac{\theta}{\pi};\quad \frac{\sin\frac{\theta}{n}}{\sin 4\alpha} = \frac{\theta}{2\pi};\ \&c.$$

$$\therefore \sin\theta = \theta\left(1 - \frac{\theta^2}{\pi^2}\right)\left(1 - \frac{\theta^2}{2^2\pi^2}\right)\left(1 - \frac{\theta^2}{3^2\pi^2}\right)\ldots$$

Similarly, $\cos\theta = \left(1 - \dfrac{4\theta^2}{\pi^2}\right)\left(1 - \dfrac{4\theta^2}{3^2\pi^2}\right)\left(1 - \dfrac{4\theta^2}{5^2\pi^2}\right)\ldots$

The same values of $\sin\theta$ and $\cos\theta$ may, of course, be obtained from the formulæ for $\sin n\theta$ and $\cos n\theta$ when n is even.

Putting $\theta = \dfrac{\pi}{2}$ in the resolution of $\sin\theta$, we get

$$1 = \frac{\pi}{2}\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{4^2}\right)\left(1 - \frac{1}{6^2}\right)\ldots\left\{1 - \frac{1}{(2n)^2}\right\},\ (n = \infty);$$

$$\therefore \frac{\pi}{2} = \frac{2.2.4.4.6.6 \quad \ldots \quad 2n.2n}{1.3.3.5.5.7 \ldots (2n-1)(2n+1)}\ (n = \infty),$$

which is Wallis's formula.

(19) If we develope these values of $\sin\theta$ and $\cos\theta$ according to ascending powers of θ, and compare the results with the common formulæ

$$\sin\theta = \theta + \frac{\theta^3}{1.2.3} + \ldots,\quad \cos\theta = 1 - \frac{\theta^2}{1.2} + \ldots,$$

we find

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\ldots=\frac{\pi^2}{6},$$

$$\frac{1}{1^2}+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\ldots=\frac{\pi^2}{8}.$$

(20) By making $x=1$ in the result of example 15, we may deduce two important formulæ: first, we have

$$2(1-\cos\theta)=2\left(1-\cos\frac{\theta}{n}\right)\,2\left(1-\cos\frac{2\pi+\theta}{n}\right)\times$$
$$2\left(1-\cos\frac{4\pi+\theta}{n}\right)\ldots 2\left(1-\cos\frac{2(n-1)\pi+\theta}{n}\right);$$

therefore, replacing $1-\cos\theta$ by $2\sin^2\frac{\theta}{2}$, &c., extracting the square root of both sides, and changing θ into 2θ, we get

$$\sin\theta=2^{n-1}\sin\frac{\theta}{n}\sin\frac{\pi+\theta}{n}\sin\frac{2\pi+\theta}{n}\ldots\sin\frac{(n-1)\pi+\theta}{n};$$

and writing $\frac{\pi}{2}+\theta$ for θ,

$$\cos\theta=2^{n-1}\sin\frac{\pi+2\theta}{2n}\sin\frac{3\pi+2\theta}{2n}\sin\frac{5\pi+2\theta}{2n}\ldots$$
$$\ldots\sin\frac{(2n-1)\pi+2\theta}{2n}.$$

The formulæ which result from these by putting $\theta=0$, are sometimes of use; they are, since in that case

$$\sin\theta\div\sin\frac{\theta}{n}=n,$$

$$n=2^{n-1}\sin\frac{\pi}{n}\sin\frac{2\pi}{n}\sin\frac{3\pi}{n}\ldots\sin\frac{(n-1)\pi}{n},$$

$$1=2^{n-1}\sin\frac{\pi}{2n}\sin\frac{3\pi}{2n}\sin\frac{5\pi}{2n}\ldots\sin\frac{(2n-1)\pi}{2n}.$$

(21) If in the expression $x^2-2rx\cos\phi+r^2$, we write $1+\frac{z}{2n}$ for x, and $1-\frac{z}{2n}$ for r, it becomes

$$\left(1+\frac{z}{2n}\right)^2-2\left(1-\frac{z^2}{4n^2}\right)\cos\phi+\left(1-\frac{z}{2n}\right)^2=2\left(1+\frac{z^2}{4n^2}\right)$$

$$-2\left(1-\frac{z^2}{4n^2}\right)\cos\phi=4\sin^2\frac{\phi}{2}\left(1+\frac{z^2}{4n^2}\cot^2\frac{\phi}{2}\right).$$

If then $\phi=\frac{2\lambda\pi\pm\theta}{n}$, the expression just found is the general form of the quadratic factor of

$$\left(1+\frac{z}{2n}\right)^{2n}-2\left(1-\frac{z^2}{4n^2}\right)^n\cos\theta+\left(1-\frac{z}{2n}\right)^{2n};$$

and this quantity therefore, taking λ from 0 to $\frac{1}{2}n$ or $\frac{1}{2}(n-1)$,

$$=4\sin^2\frac{\theta}{2n}\,.\,4\sin^2\frac{2\pi\pm\theta}{2n}\ldots$$

$$\times\left(1+\frac{z^2}{4n^2}\cot^2\frac{\theta}{2n}\right)\left(1+\frac{z^2}{4n^2}\cot^2\frac{2\pi\pm\theta}{2n}\right)\ldots$$

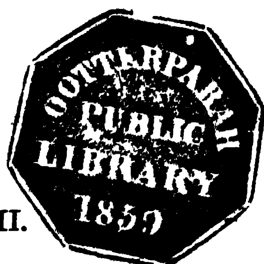
Now make $n=\infty$, observing that, in that case, $\left(1\pm\frac{z}{2n}\right)^{2n}=e^{\pm z}$ (e denoting the base of *Napier's* system of logarithms), $2n\tan\frac{\theta}{2n}=\theta$, and that, by putting $z=0$, we have

$$2\sin\frac{\theta}{2n}\,.\,2\sin\frac{2\pi\pm\theta}{2n}\ldots=2\sin\frac{\theta}{2};$$

$$\therefore\ e^z-2\cos\theta+e^{-z}$$

$$=4\sin^2\frac{\theta}{2}\left(1+\frac{z^2}{\theta^2}\right)\left\{1+\frac{z^2}{(2\pi\pm\theta)^2}\right\}\left\{1+\frac{z^2}{(4\pi\pm\theta)^2}\right\}\ldots$$

where both signs are to be taken. The particular cases of $\theta=0$, $\theta=\pi$, may be noticed. Several of the preceding results are useful in the higher branches of Mathematics, especially in the Integral Calculus.



SECTION II.

ON THE TRANSFORMATION OF EQUATIONS.

---

23. In discovering the properties of $f(x) = 0$, and determining its roots, one method of great value is to transform it into another equation, $\phi(y) = 0$, whose roots have given relations with its roots. We thus, without knowing the roots of a proposed equation, make them undergo certain changes, such as all to be increased or diminished by a given quantity, or all to be multiplied or divided by the same number; which render the determination of the roots easier, or the equation in its new form more convenient for solution.

The problem of transforming an equation is, in its most general state, to eliminate x between the equations

$$f(x) = 0, \ \psi(x, y) = 0,$$

the latter being the equation which expresses the relation which the roots of the transformed are required to have with those of the proposed equation.

At present, we shall confine ourselves to a few simple cases which are necessary in the actual solution of equations, reserving the others to the Section on Elimination.

24. To transform an equation into one whose roots are those of the proposed equation, with contrary signs.

Let $a, b, c, \ldots l$, be the roots of the equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0;$$

$$\therefore \ x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n$$
$$= (x-a)(x-b)(x-c) \ldots (x-l).$$

In this identical equation change x into $-y$; then, whether n be odd or even, the result is

$$y^n - p_1 y^{n-1} + p_2 y^{n-2} - \dots \pm p_n$$
$$= (y+a)(y+b)(y+c) \dots (y+l),$$

which shews that the first member, put equal to zero, is an equation in y, whose roots are $-a$, $-b$, $-c$, ... $-l$. Hence, if the signs of the alternate terms, beginning with the second, of any complete equation be changed, the signs of all the *roots are changed.*

Before this theorem can be applied to incomplete equations, the deficient terms must be replaced by cyphers. Thus the equation

$$x^4 - qx + r = 0, \text{ or } x^4 + 0x^3 + 0x^2 - qx + r = 0,$$

is one whose roots differ from those of $x^4 + qx + r = 0$ only in sign.

25. To transform an equation into one whose roots are those of the proposed equation, each diminished or increased by the same given quantity.

Let a, b, c, ... l, be the roots of the equation

$$x^n + p_1 x^{n-1} + \dots + p_{n-1} x + p_n = 0;$$
$$\therefore x^n + p_1 x^{n-1} + \dots + p_{n-1} x + p_n$$
$$= (x-a)(x-b)(x-c) \dots (x-l).$$

In this identical equation, change x into $y + h$;

$$\therefore (y+h)^n + p_1 (y+h)^{n-1} + \dots + p_{n-1}(y+h) + p_n$$
$$= \{y-(a-h)\}\{y-(b-h)\} \dots \{y-(l-h)\},$$

which shews that the first member, put equal to zero, is an equation in y, whose roots are $a-h$, $b-h$, ... $l-h$; or, expanding by the binomial theorem, and arranging it according to powers of y, we have the transformed equation

$$y^n + \left.\begin{matrix} nh \\ +p_1 \end{matrix}\right\} y^{n-1} + \left.\begin{matrix} \frac{n(n-1)}{2} h^2 \\ +(n-1)p_1 h \\ + \quad p_2 \end{matrix}\right\} y^{n-2} + \dots + \left.\begin{matrix} h^n \\ +p_1 h^{n-1} \\ +p_2 h^{n-2} \\ + \dots \\ +p_{n-1} h \\ +p_n \end{matrix}\right\} = 0.$$

To increase, on the contrary, all the roots, we must change x into $y-h$, and therefore we must take the odd powers of h in the above equation with a contrary sign.

26. If we arrange the transformed equation

$$(y+h)^n + p_1(y+h)^{n-1} + p_2(y+h)^{n-2} + \dots$$
$$+ p_{n-1}(y+h) + p_n = 0,$$

according to ascending powers of y, we shall see the law of formation of its coefficients more distinctly; for we then have

$$h^n + p_1h^{n-1} + p_2h^{n-2} + \dots + p_{n-2}h^2 + p_{n-1}h + p_n$$
$$+ \{nh^{n-1} + (n-1)p_1h^{n-2} + (n-2)p_2h^{n-3} + \dots$$
$$+ 2p_{n-2}h + p_{n-1}\}\,y$$
$$+ \{n(n-1)h^{n-2} + (n-1)(n-2)p_1h^{n-3} + \dots + 2p_{n-2}\}\frac{y^2}{\lfloor 2}$$
$$+ \ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \{n(n-1)\dots 3.2\}\frac{y^n}{\lfloor n} = 0,$$

where $\lfloor n$ denotes $1.2.3\dots n$.

The first coefficient is the original polynomial with h instead of x, and will therefore be represented by $f(h)$; the second coefficient is derived from the first by multiplying every term in $f(h)$ by the index of that power of h which it involves and diminishing the index by unity, and may be represented by $f'(h)$; the third is found from the second, by repeating the same process upon $f'(h)$, or performing it twice upon $f(h)$, and may therefore be represented by $f''(h)$; and in like manner all the other coefficients, being formed by the same uniform law, may be represented by $f'''(h), \dots f^{n-1}(h)$; therefore the transformed equation, arranged according to ascending powers of y, is

$$f(h) + f'(h)\,y + f''(h)\frac{y^2}{1.2} + f'''(h)\frac{y^3}{\lfloor 3} + \dots$$
$$+ f^{n-1}(h)\frac{y^{n-1}}{\lfloor n-1} + y^n = 0.$$

27. Hence it follows that if in $f(x)$ we change x into $x+h$, the result, arranged according to powers of h, is

$$f(x+h)=f(x)+f'(x)\,h+f''(x)\,\frac{h^2}{1\,.\,2}+\ldots$$

$$+f^{n-1}(x)\,\frac{h^{n-1}}{\lfloor n-1}+f^{n}(x)\,\frac{h^{n}}{\lfloor n};$$

$f'(x)$, $f''(x)$, ...$f^{n-1}(x)$ being derived from $f(x)$ according to the law explained above; they are called derived functions relative to the given function $f(x)$, or derivatives of $f(x)$.

Obs. Those who are acquainted with the Differential Calculus, know that the above result can be immediately obtained from *Taylor's* theorem; and that $f'(x)$, $f''(x)$, &c., are the first, second, &c., differential coefficients of $f(x)$, which all vanish after the n^{th}, $f(x)$ being here a rational integral function of the n^{th} degree.

28. Hence, to increase or diminish the roots of a proposed equation, $f(x)=0$, by a given quantity h, we must write down $f(x)$ and all the derived functions, $f'(x)$, $f'(x)$, $f''(x)$ ... $f^{n-1}(x)$, and substitute in them $-h$ or $+h$ for x, according as the roots are to be increased or diminished; the resulting quantities are the coefficients of the transformed equation.

Ex. 1. To transform $x^5+5x^4+x^3-16x^2-20x-16=0$, into one whose roots shall be the same, except that each is increased by unity.

Here $y=x+1$, or $x=y-1$;

therefore the transformed equation is

$$f(-1)+f'(-1)\,y+f''(-1)\,\frac{y^2}{2}+f^3(-1)\,\frac{y^3}{\lfloor 3}$$

$$+f^4(-1)\,\frac{y^4}{\lfloor 4}+y^5=0;$$

but $f(x) = x^5 + 5x^4 + x^3 - 16x^2 - 20x - 16$ $f(-1) = -9$
$f'(x) = 5x^4 + 20x^3 + 3x^2 - 32x - 20$ $f'(-1) = 0$
$f''(x) = 20x^3 + 60x^2 + 6x - 32$ $f''(-1) = 2$
$f^3(x) = 60x^2 + 120x + 6$ $f^3(-1) = -54$
$f^4(x) = 120x + 120$ $f^4(-1) = 0$;

$$\therefore\ -9 + 2 \cdot \frac{y^2}{2} - 54 \cdot \frac{y^3}{6} + y^5 = 0,$$

$$\text{or } y^5 - 9y^3 + y^2 - 9 = 0,$$

the roots of which were found (p. 17).

Ex. 2. To increase, and diminish, by 3, the roots of

$$x^3 - 2x^2 - x + 2 = 0.$$

The transformed equations are

$$y^3 - 11y^2 + 38y - 40 = 0,\ y^3 + 7y^2 + 14y + 8 = 0.$$

29. One use of this transformation is to take away any term of an equation; by which means it is sometimes reduced to a form more convenient for solution, as in the former of the preceding Example.

Thus, to transform $f(x) = 0$ into one which shall want the second term, we must have (Art. 25) $nh + p_1 = 0$, or $h = -\frac{p_1}{n}$, and therefore $x = y - \frac{p_1}{n}$; i.e., the roots must be increased by $\frac{p_1}{n}$, p_1 being the coefficient of the second term with its proper sign, and n the degree of the equation. We may arrive at this result immediately, by observing that if $a, b, c, \ldots l$ be the roots of $x^n + p_1 x^{n-1} + \ldots = 0$, and $a + h$, $b + h, \ldots l + h$ those of the transformed equation $y^n + q_1 y^{n-1} + \ldots = 0$, then $-q_1 = a + b + \ldots l + nh = -p_1 + nh$; and if this $= 0$, then $h = \frac{p_1}{n}$, the quantity by which the roots are to be increased.

To take away the third term, we must diminish the roots by a quantity h determined from the equation (Art. 25)

$$\frac{n(n-1)}{2}h^2+(n-1)p_1h+p_2=0;$$

and, in general, to take away the $(r+1)^{\text{th}}$ term, we must diminish the roots by a quantity h determined from the equation (Art. 26)

$$f^{n-r}(h)=0, \text{ or } h^r+\frac{r}{n}p_1h^{r-1}+\frac{r(r-1)}{n(n-1)}p_2h^{r-2}+\ldots=0.$$

To take away the last term, we must have

$$h^n+p_1h^{n-1}+\ldots=0;$$

i.e., we must solve the original equation. In effect, the transformed equation would have one root $=0$, and therefore $h=x$.

Obs. If all the roots of $f(x)=0$ be real, it will be seen further on that all those of $f^{n-r}(x)=0$ are so; therefore the equation may be transformed in r different ways so as to want the $(r+1)^{\text{th}}$ term; but if all the roots of $f^{n-r}(x)=0$ be impossible, in which case its dimension r must be even, $f(x)=0$ cannot be transformed into another with real coefficients so as to want the $(r+1)^{\text{th}}$ term; and in the latter case, the proposed equation will have at least r imaginary roots.

Ex. 1. To transform $x^3-6x^2+4x-7=0$ into one which shall want the second term.

Here $p_1=-6$, $n=3$; $\therefore\ x=y-\frac{p_1}{n}=y+2$;

$$\therefore\ (y+2)^3-6(y+2)^2+4(y+2)-7=0,$$
$$\text{or } y^3-8y-15=0.$$

Ex. 2. To transform $x^3+5x^2+8x-1=0$ into two others which shall each want the third term. The transformed equations are

$$y^3-y^2-5=0,\ y^3+y^2-\frac{139}{27}=0.$$

30. To transform an equation into another, of which the roots are equal to those of the proposed, each multiplied by the same given quantity.

In the identical equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \dots + p_{n-1}x + p_n$$
$$= (x-a)(x-b) \dots (x-l),$$

change x into $\frac{y}{m}$, and then multiply both sides by m^n,

$$\therefore\ y^n + mp_1 y^{n-1} + m^2 p_2 y^{n-2} + \dots + m^{n-1}p_{n-1}y + m^n p_n$$
$$= (y-ma)(y-mb) \dots (y-ml);$$

therefore the roots of

$$y^n + mp_1 y^{n-1} + m^2 p_2 y^{n-2} + \dots + m^{n-1}p_{n-1}y + m^n p_n = 0,$$

are ma, mb, mc, ... ml; and it is formed from the equation, supposed complete, whose roots are a, b, c, ... l, by multiplying the coefficients, beginning with that of the second term, by m, m^2, m^3, ... m^n.

The use of this transformation is to get rid of the coefficient of the first term; or to make the fractional coefficients of an equation disappear, without affecting the first term with any coefficient except unity.

Thus, if $mx^n + p_1 x^{n-1} + p_2 x^{n-2} + \dots = 0$ have roots a, b, c, &c.,

$$\text{then } my^n + mp_1 y^{n-1} + m^2 p_2 y^{n-2} + \dots = 0$$
$$\text{or } y^n + p_1 y^{n-1} + mp_2 y^{n-2} + \dots = 0$$

has roots ma, mb, mc, &c., and is of the usual form.

Also, if $x^n + \frac{p_1}{q_1}x^{n-1} + \frac{p_2}{q_2}x^{n-2} + \frac{p_3}{q_3}x^{n-3} + \dots = 0$ have roots a, b, c, &c.; and if m be the least common multiple of all the denominators q_1, q_2, q_3, &c., then

$$y^n + \frac{mp_1}{q_1}y^{n-1} + \frac{m^2 p_2}{q_2}y^{n-2} + \dots = 0$$

has roots ma, mb, mc, &c., and all its coefficients are integers.

Similarly, an equation may be transformed into another of which the roots are equal to those of the proposed, each

divided by the same given quantity, by dividing the second, third, fourth terms, &c. (supposing the equation complete) by m, m^2, m^3, &c. respectively.

31. By taking $m =$ the least common multiple of the denominators, we do not always get the transformed equation with coefficients the least possible. All that is necessary is to determine m so that m, m^2, m^3 ... are divisible respectively by q_1, q_2, q_3, ...; and therefore that m, m^2, m^3, &c. contain the prime factors of q_1, q_2, q_3, ... raised at least to as high powers as they occur in the respective denominators.

Ex. 1. $$x^3 - \frac{4}{3}x^2 - \frac{3}{8}x + \frac{5}{72} = 0.$$

The transformed equation is

$$y^3 - m\frac{4}{3}y^2 - m^2\frac{3}{2^3}y + m^3\frac{5}{3^2.2^3} = 0,$$

and the factors which the successive terms require in m are 3, 2^2, 3.2, which is satisfied by $m = 12$; and the transformed equation becomes

$$y^3 - 16y^2 - 54y + 120 = 0, \text{ where } y = 12x.$$

Ex. 2. $$x^4 - \frac{5}{6}x^3 + \frac{5}{12}x^2 - \frac{7}{150}x - \frac{13}{900} = 0.$$

The transformed equation is

$$y^4 - 25y^3 + 375y^2 - 1260y - 11700 = 0, \text{ where } y = 30x.$$

32. To transform an equation into one whose roots are the reciprocals of the roots of the proposed equation.

If in the identical equation

$$x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n = (x-a)(x-b)\ldots(x-l),$$

we change x into $\frac{1}{y}$, we get

$$\frac{1}{y^n}+\frac{p_1}{y^{n-1}}+\ldots+\frac{p_{n-1}}{y}+p_n=\left(\frac{1}{y}-a\right)\left(\frac{1}{y}-b\right)\ldots\left(\frac{1}{y}-l\right)$$

$$=\frac{-a}{y}\left(y-\frac{1}{a}\right).\frac{-b}{y}\left(y-\frac{1}{b}\right)\ldots$$

$$=\frac{p_n}{y^n}\left(y-\frac{1}{a}\right)\left(y-\frac{1}{b}\right)\ldots\left(y-\frac{1}{l}\right),$$

$$\text{or } y^n+\frac{p_{n-1}}{p_n}y^{n-1}+\frac{p_{n-2}}{p_n}y^{n-2}+\ldots+\frac{p_1}{p_n}y+\frac{1}{p_n}$$

$$=\left(y-\frac{1}{a}\right)\left(y-\frac{1}{b}\right)\ldots\left(y-\frac{1}{l}\right);$$

which shews that if we write $\frac{1}{y}$ for x, and then multiply by y^n, the resulting expression put $=0$, has roots $\frac{1}{a}, \frac{1}{b}, \ldots \frac{1}{l}$.

33. This transformation fails if the transformed equation be identical with the original one; that is, if the coefficients be such that

$$p_{n-1}=p_n p_1,\; p_{n-2}=p_n p_2,\; \&c.,\; 1=p_n p_n.$$

Hence $p_n=\pm 1$; and according as we take the upper or lower sign, we have

$$p_{n-1}=p_1,\; p_{n-2}=p_2,\; \&c.;$$

$$\text{or, } p_{n-1}=-p_1,\; p_{n-2}=-p_2,\; \&c.$$

that is, the coefficients of corresponding terms taken from the beginning and end must be equal and of the same signs; or, they must be equal and of contrary signs; only it must be observed that if the equation be of an even number of dimensions $2r$, there will be a middle term $p_r x^r$, and we shall have $p_r=p_r p_{2r}$; which, for $p_{2r}=-1$, gives

$$p_r=-p_r, \text{ or } p_r=0;$$

so that when the equation is of an even degree and the corresponding coefficients have contrary signs, there must be no middle term.

It is easy to see that when these conditions are satisfied, the equation remains the same when $\frac{1}{x}$ is substituted for x; *but when the corresponding coefficients have contrary signs* it will be necessary, after the substitution, to change the signs of all the terms; and the above investigation shews that these are the only conditions under which an equation can have the property. Equations of this sort, that is, which remain the same when x is changed into $\frac{1}{x}$, are called Reciprocal Equations.

34. Every reciprocal equation will have its roots in pairs a, $\frac{1}{a}$, b, $\frac{1}{b}$, &c.; but when the degree is odd, there will, besides, be a root $+1$ or -1, according as the last term is negative or positive; and when the degree is even with the last term negative, there will be two roots $+1$ and -1.

For if a be a root of the proposed equation, $\frac{1}{a}$ will be a root of the transformed equation; but the transformed equation coincides with the proposed, therefore $\frac{1}{a}$ will be a root of the proposed equation; and so on for every other root. Also, since 1 and -1 are the same as their reciprocals, each of these may enter any even number of times.

Again, we may write the reciprocal equation of an odd degree, collecting the terms from the beginning and end,

$$x^n \pm 1 + p_1 x (x^{n-2} \pm 1) + \ldots = 0;$$

and since every term is divisible by $x \pm 1$, it will have a root $+1$ or -1 according as its last term is negative or positive.

Also, the reciprocal equation of an even degree with its last term negative may be written

$$x^n - 1 + p_1 x (x^{n-2} - 1) + \ldots = 0,$$

which is divisible by x^2-1; therefore it has two roots $+1$ and -1.

In both cases, when the factor $x \pm 1$ or x^2-1 is expelled, the equation is reduced to a reciprocal equation of an even degree with its last term positive, which may therefore be taken as the standard form of reciprocal equations.

Ex. Reduce to a reciprocal equation of an even degree with its last term positive, each of the equations

$$x^5 - \frac{1}{6}x^4 - \frac{43}{6}x^3 + \frac{43}{6}x^2 + \frac{1}{6}x - 1 = 0,$$

$$x^6 + \frac{5}{6}x^5 - \frac{22}{3}x^4 + \frac{22}{3}x^2 - \frac{5}{6}x - 1 = 0.$$

---

35. Various transformations may be effected by particular artifices; we shall give one or two instances, of which the results will be useful to us in the sequel, and are of importance in discovering the existence of impossible roots in equations.

(1) To transform an equation into one whose roots are the squares of the roots of the proposed.

If $\quad x^n + p_1x^{n-1} + p_2x^{n-2} + p_3x^{n-3} + \ldots + p_{n-1}x + p_n$
$$= (x-a)(x-b)\ldots(x-l),$$
then $\quad x^n - p_1x^{n-1} + p_2x^{n-2} - p_3x^{n-3} + \ldots \pm p_{n-1}x \mp p_n$
$$= (x+a)(x+b)\ldots(x+l); \quad \text{(Art. 24)}$$
therefore, multiplying these equations together, we get

$$(x^n + p_2x^{n-2} + p_4x^{n-4} + \ldots)^2 - (p_1x^{n-1} + p_3x^{n-3} + \ldots)^2$$
$$= (x^2-a^2)(x^2-b^2)\ldots(x^2-l^2);$$

but the first member is

$$x^{2n} + 2p_2x^{2n-2} + (2p_4 + p_2^2)x^{2n-4} + \ldots$$
$$- (p_1^2x^{2n-2} + 2p_1p_3x^{2n-4} + \ldots);$$

therefore, replacing x^2 by y, we have

$$y^n + (2p_2 - p_1^2)\,y^{n-1} + (p_2^2 - 2p_1p_3 + 2p_4)\,y^{n-2} + \ldots$$
$$= (y - a^2)\,(y - b^2)\ldots(y - l^2);$$

hence the transformed equation, whose roots are a^2, b^2, &c., is

$$y^n + (2p_2 - p_1^2)\,y^{n-1} + (p_2^2 - 2p_1p_3 + 2p_4)\,y^{n-2} + \ldots = 0.$$

Hence the proposed equation (since its roots are the square roots of those of the transformed equation) cannot have more real roots than the latter has positive roots.

Ex. $$x^5 + x^3 + 3x^2 + 16x + 15 = 0.$$

The transformed equation is

$$x^5 + 2x^4 + 33x^3 + 23x^2 + 166x - 225 = 0,$$

which (Art. 11) has only one positive root; and therefore the proposed has only one real root.

(2) To transform the equation $x^3 + qx + r = 0$ into one whose roots are the squares of the differences of its roots.

Let the roots of $x^3 + qx + r = 0$ be a, b, c;

$$\therefore\ 0 = a + b + c,\quad q = ab + ac + bc,\quad -r = abc,$$
$$\text{and}\ \ a^2 + b^2 + c^2 = -2q,\ \text{(Art. 21)}.$$

Since one root of the transformed equation is

$$(a - b)^2 = a^2 + b^2 + c^2 - c^2 - \frac{2abc}{c} = -2q - c^2 + \frac{2r}{c},$$

if we assume $y = -2q - x^2 + \frac{2r}{x}$, then when x assumes its three values, y becomes equal to the three roots of the transformed equation; therefore the required equation will result from eliminating x between the proposed and

$$x^3 + (y + 2q)\,x - 2r = 0;$$

subtracting this from the proposed, we have

$$(y + q)\,x - 3r = 0,\ \text{or}\ x = \frac{3r}{y + q};$$

and if we substitute this value, and reduce, we obtain the transformed equation

$$y^3 + 6qy^2 + 9q^2y + 108\left(\frac{r^2}{4} + \frac{q^3}{27}\right) = 0.$$

Hence, if $\frac{r^2}{4} + \frac{q^3}{27}$ is positive, the transformed has a real negative root (Art. 10), and therefore the proposed equation must have a pair of imaginary roots; since it is only when two roots are imaginary and conjugate to one another, that the square of their difference can be negative.

If $\frac{r^2}{4} + \frac{q^3}{27} = 0$, then one value of y is zero; and therefore the proposed has a pair of equal roots.

If $\frac{r^2}{4} + \frac{q^3}{27}$ is negative (and therefore q an essentially negative quantity) the transformed equation cannot have a negative root (Art. 3); and therefore the proposed has all its roots real.

Ex. $$x^3 - 7x + 7 = 0.$$

The equation of differences is

$$y^3 - 42y^2 + 441y - 49 = 0,$$

which cannot have a negative root (Art. 3); therefore the proposed has all its roots real.

SECTION III.

ON THE LIMITS OF THE ROOTS OF EQUATIONS.

---

36. THE limits of any group of roots of an equation are two quantities between which the whole group lies; thus $+\infty$ and 0 are limits of the positive roots of every equation, and 0 and $-\infty$ of the negative roots. But in practice we are required to assign much closer limits than these, usually the two consecutive whole numbers between which each root lies, so that the inferior limit is the integral part of the included root. This may be effected without knowing any of the roots of the equation, as will be seen in the following propositions. The roots spoken of in this section are the real roots.

37. Quantities between which the real roots of an equation taken in order lie, when substituted successively for the unknown quantity, give results alternately positive and negative.

Let the real roots, arranged in order of magnitude, be $a, b, c, \ldots l$, so that a is greater than b, b greater than c, &c.; the negative roots, if there be any, coming at the end of the series, and that being the least whose numerical value (neglecting the sign) is the greatest; then if $f(x) = 0$ be the equation,

$$f(x) = (x - a)(x - b)(x - c) \ldots (x - l) \cdot \phi(x),$$

where $\phi(x)$ is a polynomial that remains positive whatever real values be substituted in it for x, (Art. 15). Then if we substitute for x a quantity α greater than a, the result $f(\alpha)$ is positive because every one of its factors is so; if we

substitute a quantity β between a and b, the *result* $f(\beta)$ is negative because the first factor is negative and the rest positive. Again, a quantity between b and c renders the whole positive, because the *two first factors are negative* and the rest positive. Thus, quantities between which the roots taken in order lie, when substituted for x, give results alternately positive and negative.

38. Again, suppose that $a, b, c, \ldots l$ are all the roots of $f(x)=0$, which lie between two numbers α and β, of which α is the lesser, and that $\phi(x)=0$ is the equation containing the remaining roots; then substituting α and β successively for x, and dividing one result by the other, we get

$$\frac{f(\alpha)}{f(\beta)}=\frac{(\alpha-a)(\alpha-b)\ldots(\alpha-l)}{(\beta-a)(\beta-b)\ldots(\beta-l)}\cdot\frac{\phi(\alpha)}{\phi(\beta)}.$$

Now all the factors in the numerator are negative, and all in the denominator positive; also $\phi(\alpha)$, $\phi(\beta)$, must have the same sign, since $\phi(x)=0$ has no root between α and β; therefore $f(\alpha)$, $f(\beta)$ have different, or the same signs, according as the number of factors $\alpha-a$, $\alpha-b$, &c. is odd or even.

Hence if two numbers, when substituted for x, give results with different signs, then one, three, or some odd number of roots lies between them; if they give results with the same sign, then two, four, or some even number of roots lies between them, or none at all.

39. If a number α can be found such that α and every greater number, when substituted for x, gives a finite positive result, then α is greater than the greatest root, and is called a superior limit of the roots; for if there could be a root greater than α, then some number greater than α would give a negative result, which is contrary to the supposition. Similarly, if a number β can be found such that β and every smaller number, when substituted for x, gives a finite result with a permanent sign, that is, constantly positive or con-

stantly negative, according as the degree of the equation is even or odd, β is less than the least root, and is called an inferior limit of the roots.

Obs. This supposes the greatest and least roots to occur singly; or, if repeated, to be repeated an odd number of times; for if we had

$$f(x) = (x-a)^2 (x-b) \ldots,$$

and α were between a and b, then α and every greater number would give a positive result, without α being the superior limit.

40. If as many quantities can be found, which, substituted for x in $f(x)$, give results alternately positive and negative, as the equation has dimensions, it is plain that the odd number of roots which lies between each adjacent two of the quantities, cannot exceed one. But as it is seldom the case that so many can be found, the next point to be determined is, whether all the real roots that exist have been discovered; this enquiry will obviously be narrowed if we find the limits beyond which the quantities, successively substituted for the purpose of separating the roots, need not extend, that is, the superior and inferior limits of the positive and negative roots; the principal methods of doing this are the following.

SUPERIOR AND INFERIOR LIMITS OF THE ROOTS.

41. All the roots of an equation lie between $p+1$ and $-(p+1)$, p being the greatest coefficient without regard to sign.

For it is proved (Art. 9) that $p+1$ and every greater number, when substituted for x, gives a positive result, therefore $p+1$ is greater than the greatest root; also that $-(p+1)$ and every greater negative number gives a result with a permanent sign, that is, constantly positive or constantly negative, according as the degree of the equation is even or odd, therefore $-(p+1)$ is less than the least root.

42. The greatest negative coefficient increased by unity, is a superior limit of the positive roots of an equation.

Let $-p$ be the greatest negative coefficient; then any value of x which makes

$$x^n - p\,(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1) \text{ positive,}$$

$$\text{or } x^n > p\,(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1) > p\,\frac{x^n - 1}{x - 1},$$

will, *a fortiori*, make

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n \text{ positive,}$$

or make $f(x)$ positive; because in the latter case there will generally be fewer terms to be taken away from x^n; and of these, not one is greater than the corresponding term in the former case.

Now the inequality $x^n > p\,\dfrac{x^n - 1}{x - 1}$, is satisfied if

$$x^n = \text{or} > x^n \frac{p}{x-1}, \text{ or } x - 1 = \text{or} > p, \text{ or } x = \text{or} > p + 1.$$

Since, therefore, $p + 1$ and every greater number, when substituted for x, will make $f(x)$ positive, the numerical value of the greatest negative coefficient increased by unity, is a superior limit of the positive roots.

Obs. This result, as is easily seen, is included in that of the preceding article; for if all the coefficients were negative, the substitution of the greatest of them increased by unity, and of every greater quantity, would give a positive result; therefore, *a fortiori*, the result will be positive if some of the coefficients be positive; the limit however here determined will usually be less than that in the former article, and never greater.

43. In any equation, if $p_r x^{n-r}$ be the first negative term, and $-p$ the greatest negative coefficient, $1 + \sqrt[r]{p}$ is a superior limit of the positive roots.

Any value of x which makes

$$x^n > p\,(x^{n-r} + x^{n-r-1} + \dots + x + 1) > p\,\frac{x^{n-r+1} - 1}{x - 1},$$

will of course make $x^n + p_1x^{n-1} + p_2x^{n-2} + \dots$ positive.

Now the inequality $x^n > p\,\dfrac{x^{n-r+1} - 1}{x - 1}$, is satisfied if

$$x^n > p\,\frac{x^{n-r+1}}{x-1},\ \text{or}\ x^{r-1}(x-1) > p,\ \text{or}\ (x-1)^{r-1}(x-1) = \text{or} > p,$$

$$\text{or}\ (x-1)^r = \text{or} > p,\ \text{or}\ x = \text{or} > 1 + \sqrt[r]{p}.$$

Since, therefore, $1 + \sqrt[r]{p}$ and every greater number gives a positive result, $1 + \sqrt[r]{p}$ is a superior limit.

This method may be employed when the first term is followed by one or more positive terms.

Ex. $$x^4 + 11x^2 - 25x - 61 = 0.$$

Here $r = 3$, and a limit of the positive roots

$$= 1 + \sqrt[3]{61} = 5.$$

44. If each negative coefficient, taken positively, be divided by the sum of all the positive coefficients which precede it, the greatest of the fractions thus formed, increased by unity, is a superior limit of the positive roots.

Let the equation be

$$x^n + p_1x^{n-1} + p_2x^{n-2} + (-p_3)\,x^{n-3} + \dots$$
$$\dots + (-p_r)\,x^{n-r} + \dots + p_n = 0;$$

then, since (Art. 5)

$$p_mx^m = p_m\,(x-1)\,(x^{m-1} + x^{m-2} + \dots + x + 1) + p_m,$$

if we transform every positive term by this formula, and leave the negative terms in their original form, we shall have

$$0 = (x-1)x^{n-1} + (x-1)x^{n-2} + (x-1)x^{n-3} + \ldots + x - 1 + 1$$
$$+ p_1(x-1)x^{n-2} + p_1(x-1)x^{n-3} + \ldots + p_1(x-1) + p_1$$
$$+ p_2(x-1)x^{n-3} + \ldots + p_2(x-1) + p_2$$
$$- p_3 x^{n-3}$$
$$+ \ldots\ldots\ldots\ldots$$

Now if such a value be assigned to x that every term is positive, that value will be the superior limit required; in the terms where no negative coefficient enters, it is sufficient to have $x > 1$; in the other terms, each of which involves a negative coefficient, we must have

$$(1 + p_1 + p_2)(x-1) > p_3,$$
$$(1 + p_1 + p_2 + \ldots + p_{r-1})(x-1) > p_r, \text{ \&c.},$$

$$\text{or } x > \frac{p_3}{1 + p_1 + p_2} + 1; \; x > \frac{p_r}{1 + p_1 + p_2 + \ldots + p_{r-1}} + 1; \text{ \&c.}$$

If then x be taken equal to the greatest of these fractions increased by unity, this value, and every greater value, will make $f(x)$ positive, and therefore will be a superior limit of the positive roots. This method gives a limit easily calculated, and generally not far from the truth.

Ex. 1. $\quad 4x^5 - 8x^4 + 23x^3 + 105x^2 - 80x + 3 = 0.$

The fractions are $\frac{8}{4}$ and $\frac{80}{4 + 23 + 105}$, and $\frac{8}{4} > \frac{80}{132}$; therefore 3 is a superior limit.

Ex. 2. $\quad 4x^7 - 6x^6 - 7x^5 + 8x^4 + 7x^3 - 23x^2 - 22x - 5 = 0$; here 3 is a superior limit.

Obs. The form of the equation will often suggest artifices, by means of which closer limits may be determined than by any of the preceding methods; thus, writing the equation of Ex. 1 under the form

$$4x^4(x-2) + 23x^3 + 105x\left(x - \frac{16}{21}\right) + 3 = 0,$$

we see that $x =$ or > 2 gives a positive result, therefore 2 is a superior limit. Similarly, by writing the example of Art. 43 under the form

$$x(x^3 - 25) + 11\left(x^2 - \frac{61}{11}\right) = 0,$$

we see that 3 is a superior limit.

We have seen (Art. 12) that an equation of an even number of dimensions with its last term positive may have no real root; but we shall now shew that in any equation whatever, if the absolute term be small compared with the other terms, there will be at least one real root also very small.

45. In the equation

$$p_0 x^n + p_1 x^{n-1} + \&c. + x - r = 0,$$

where r is essentially positive, and which may represent any equation whatever, if $r < \dfrac{1}{4(1+p)}$, where p is numerically the greatest coefficient, then there is a real positive root $< 2r$.

By dividing by the coefficient of x, and changing the signs of all the terms, and of all the roots if necessary, every equation may be reduced to the form

$$-r + x + \&c. + p_1 x^{n-1} + p_0 x^n = 0 \text{ ...... (1)},$$

where r is essentially positive; let p be numerically the greatest coefficient, then any value of $x < 1$ which makes

$$-r + x > p(x^2 + x^3 + \&c. + x^n) > \frac{px^2(1 - x^{n-1})}{1 - x},$$

will make the first member of (1) positive; and this condition is fulfilled by

$$-r + x = \text{or} > \frac{px^2}{1-x},$$

$$\text{or } (1+p)x^2 - (1+r)x + r = 0,$$

$$\text{or } 2(1+p)x = (1+r) - \sqrt{(1+r)^2 - 4r(1+p)};$$

if then $4r(1+p) < 1$, the radical will have a real value $> r$; and there will be for x a real value less than $\frac{1}{2(1+p)}$ which makes the first member of (1) positive; and $x = 0$ makes it negative; therefore in any equation reduced to the above form, if $r < \frac{1}{4(1+p)}$ there is a real small positive root $< 2r$.

Ex. $x^4 + 18x^3 - 21x^2 - 12x + 1 = 0$ has a real root between 0 and $\frac{1}{6}$.

46. To find an inferior limit of the positive roots, we must transform the equation into one whose roots are the reciprocals of the roots of the proposed equation; and the reciprocal of the superior limit of the roots of the transformed equation, found by the preceding methods, will be the quantity required.

Hence if p_r denote the greatest coefficient of a contrary sign to the last term p_n, an inferior limit of the positive roots is $\frac{p_n}{p_n + p_r}$. For the transformed equation will be (Art. 32)

$$y^n + \frac{p_{n-1}}{p_n} y^{n-1} + \ldots + \frac{p_r}{p_n} y^r + \ldots + \frac{1}{p_n} = 0,$$

of which $\frac{p_r}{p_n}$ is the greatest negative coefficient; therefore $\frac{p_r}{p_n} + 1$ is a superior limit of its roots; and consequently $\frac{p_n}{p_r + p_n}$ an inferior limit of the positive roots of the proposed equation.

Ex. $$x^3 - 42x^2 + 441x - 49 = 0.$$

Here $p_n = 49$, $p_r = 441$, $\therefore \frac{49}{49 + 441}$, or $\frac{1}{10}$ is an inferior limit of the positive roots. By putting $x = \frac{1}{y}$, we may dis-

cover a limit closer to the roots; for the transformed equation is

$$y^3 - 9y^2 + \frac{6}{7}y - \frac{1}{49} = 0, \text{ or } y^2(y-9) + \frac{6}{7}\left(y - \frac{1}{42}\right) = 0,$$

which evidently has 9 for the superior limit of its positive roots, and therefore the proposed has $\frac{1}{9}$ for the inferior limit of its positive roots.

47. To find superior and inferior limits of the negative roots, we must transform the equation into one whose roots are those of the former with contrary signs (Art. 24); and if α, β, be limits, found as above, of the positive roots of this equation, then $-\alpha$ and $-\beta$ will be limits of the negative roots of the proposed equation.

Ex. $$x^3 - 7x + 7 = 0;$$

putting $x = -y$, we get $y^3 - 7y - 7 = 0$,

of which $1 + \sqrt{7}$ or 4 is a superior limit.

Also, putting $y = \frac{1}{z}$, we get $z^3 + z^2 - \frac{1}{7} = 0$,

or $z^3 - \frac{1}{28} + z^2 - \frac{3}{28} = 0$, of which $\frac{1}{3}$ is a superior limit; therefore the negative root of the proposed lies between -4, and -3.

NEWTON'S METHOD OF FINDING LIMITS OF THE ROOTS.

The limits however, deduced by any of the preceding methods, seldom approach very near to the roots; the tentative method, depending upon the following proposition, will furnish us with limits which lie much nearer to them.

48. Every number which, written for x. makes $f(x)$ and all its derived functions positive, is a superior limit of the positive roots.

For if we diminish the roots a, b, c, &c., of $f(x) = 0$ by h, that is, (Art. 25) substitute $y + h$ for x, the result is

$$f(y+h) = 0,$$

$$\text{or } f(h) + f'(h)\frac{y}{1} + f''(h)\frac{y^2}{1.2} + \ldots + f^{n-1}(h)\frac{y^{n-1}}{\lfloor n-1} + y^n = 0.$$

Now if we give such a value to h that all the coefficients of this equation are positive, then every value of y is negative; that is, all the quantities $a-h$, $b-h$, $c-h$, &c., are negative, and therefore h is greater than the greatest of the quantities a, b, c, &c., or is a superior limit of the roots of the proposed equation. Similarly, h will be an inferior limit to all the roots, provided the transformed equation be complete and its coefficients alternately positive and negative.

Ex. To find a superior limit of the roots of

$$x^3 - 5x^2 + 7x - 1 = 0.$$

The transformed equation, putting $y + h$ for x, is

$$(h^3 - 5h^2 + 7h - 1) + (3h^2 - 10h + 7)\,y + (6h - 10)\frac{y^2}{2} + y^3 = 0;$$

in which, if 3 be put for h, all the coefficients are positive, therefore 3 is a superior limit of the positive roots. Also if $\frac{1}{7}$ be put for h, the transformed equation is complete and has its terms alternately positive and negative, therefore $\frac{1}{7}$ is an inferior limit of the roots.

Obs. This method of finding a superior limit of the roots by determining by trial what value of x will make $f(x)$ and all its derived functions positive, was proposed by *Newton*.

WARING'S METHOD OF SEPARATING THE ROOTS.

49. If a series of quantities be substituted for x in $f(x)$, then between every two which give results with different

signs an odd number of roots of $f(x) = 0$ is situated; and between every two which give results with the same signs an even number is situated, or none at all; but we cannot assure ourselves that in the former case the number does not exceed unity, or that in the latter it is zero, and that consequently the number and situation of all the real roots is ascertained, unless the difference between the quantities successively substituted be less than the least difference between the roots of the proposed equation; since, if it were greater, it is evident that more than one root might be intercepted by two of the quantities giving results with different signs, and that two roots instead of none might be intercepted by two of the quantities giving results with the same sign; and in both cases, roots would pass undiscovered. We must therefore first find a limit less than the least difference of the roots; this may be done by transforming (as we have already shewn for a cubic, and shall hereafter shew generally) the equation into one whose roots are the squares of the differences of the roots of the proposed equation. Then if we find a limit k less than the least positive root of the transformed equation, $\sqrt{k}$ will be less than the least difference of the roots of the proposed equation; and if we substitute successively for x the numbers s, $s - \sqrt{k}$, $s - 2\sqrt{k}$, &c., (s being a superior limit of the roots of the proposed) till we come to a superior limit of the negative roots, we are sure that no two real roots, lying between the numbers substituted, have escaped us; and that every change of signs in the results of the substitutions indicates only one real root. Hence the number of real roots will be known (for it will exactly equal the number of changes), as well as the interval in which each of them is contained.

Obs. This method of determining the number and situation of the real roots of an equation was first proposed by *Waring;* it is however of no practical use for equations of a degree exceeding the fourth, on account of the great labour of

forming for any equation of a higher order the equation whose roots are the squares of the differences of its roots.

Ex. $x^3 - 7x + 7 = 0$. The numbers 1 and 2 give each a positive result, but yet two roots lie between them. The equation whose roots are the squares of the differences is (p. 45)

$$y^3 - 42y^2 + 441y - 49 = 0,$$

an inferior limit of the positive roots of which is $\frac{1}{9}$ (Art. 46); therefore $\frac{1}{3}$ is less than the least difference of the roots of

$$x^3 - 7x + 7 = 0,$$

and substituting $2, \frac{5}{3}, \frac{4}{3}$, the results are $+, -, +$; hence one value of x lies between 2 and $\frac{5}{3}$, and one between $\frac{5}{3}$ and $\frac{4}{3}$; and, similarly, we find the negative root, which necessarily exists, to lie between 3 and $3\frac{1}{3}$.

USE OF THE DERIVED FUNCTIONS IN FINDING LIMITS OF THE ROOTS.

50. The first derived function $f'(x)$ put equal to zero, gives an equation whose roots have remarkable relations with the roots of $f(x) = 0$; these relations we now proceed to investigate, as well as to draw several important conclusions from them, beginning with the following proposition.

51. An odd number of the roots of the equation

$$f'(x) = nx^{n-1} + (n-1)p_1x^{n-2} + (n-2)p_2x^{n-3} + \dots + p_{n-1} = 0,$$

lies between each adjacent two of the roots of $f(x) = 0$.

Let the real roots of $f(x) = 0$, arranged in descending order of magnitude, be $a, b, c, \dots l$, in number $n - r$;

$$\therefore f(x) = (x-a)(x-b)(x-c)\dots(x-l) \cdot \phi(x),$$

where $\phi(x)$ is a polynomial of r dimensions that cannot become negative for any real value of x.

In this identical equation, for x write $y+h$;

$$\therefore f(y+h) = (y+h-a)(y+h-b)(y+h-c)\ldots$$
$$\ldots(y+h-l).\phi(y+h),$$

$$\text{or } f(h) + f'(h).\frac{y}{1} + f''(h)\frac{y^2}{1.2} + \ldots + y^n$$

$$= [y^{n-r} + \ldots + \{(h-b)(h-c)\ldots + (h-a)(h-c)\ldots$$
$$\ldots + (h-a)(h-b)\ldots + \ldots\}y + (h-a)(h-b)\ldots(h-l)]$$
$$\times\{\phi(h) + \phi'(h).\frac{y}{1} + \phi''(h)\frac{y^2}{1.2} + \ldots + y^r\};$$

therefore, equating coefficients of y, which in the first member is $f'(h)$, and in the second member is the sum of the products of the constant term in each factor by the term in the other factor involving only the first power of y, we get

$$f'(h) = \{(h-b)(h-c)\ldots + (h-a)(h-c)\ldots + (h-a)(h-b)\ldots + \ldots\}$$
$$\times\phi(h) + (h-a)(h-b)\ldots(h-l)\phi'(h);$$

the coefficient of $\phi(h)$ being the sum of a series of products, in forming which, each of the factors $h-a$, $h-b$, &c. is left out in turn.

In this equation, if a, b, c, &c., be written for h, since the last term of the second member vanishes by these substitutions, and $\phi(h)$ is always positive, the results will have the same signs as

$$(a-b)(a-c)\ldots,\ (b-a)(b-c)\ldots,\ (c-a)(c-b)\ldots,\ \&c.$$

which are alternately positive and negative, since they respectively involve 0, 1, 2, ... negative factors; a, b, c, ... being arranged in order of magnitude.

Hence an odd number of roots of $f'(h) = 0$, or of

$$f'(x) = nx^{n-1} + (n-1)p_1x^{n-2} + \ldots = 0,$$

(since it is of no importance by what symbol we represent the unknown quantity,) lies between a and b, an odd number between b and c, and so on; that is, an odd number of the roots of $f'(x) = 0$, lies between each adjacent two of the roots of $f(x) = 0$.

52. If the equation $f(x) = 0$ has n real roots, then

$$nx^{n-1} + (n-1)p_1x^{n-2} + \ldots = 0, \text{ or } f'(x) = 0,$$

has $n-1$ real roots, for one of its roots lies between each adjacent two of the roots of $f(x)=0$; and it is therefore in this case called the limiting equation of the proposed.

53. The equation $f''(x) = 0$, or

$$n(n-1)x^{n-2} + (n-1)(n-2)p_1x^{n-3} + \ldots = 0,$$

being derived from $f'(x) = 0$ in the same manner as this latter is derived from $f(x) = 0$, will have an odd number of roots lying between each adjacent two of the roots of $f'(x) = 0$; and if all the roots of $f(x) = 0$ are real, all in

$$f'(x) = 0, \quad f''(x) = 0, \text{ \&c.},$$

are real, till we arrive at a simple equation. And, in general, the equations

$$f'(x) = 0, \quad f''(x) = 0, \text{ \&c.},$$

have at least as many real roots wanting one, two, &c., as $f(x) = 0$.

Hence if $f(x) = 0$ has $n-r$ possible, and r impossible roots, $f^m(x) = 0$ will have at least $n-r-m$ possible, and therefore (being of $n-m$ dimensions) cannot have more than r impossible roots; which shews that though $f(x) = 0$ may have fewer real roots than several of its derived equations, it has at least as many impossible roots as any one of them.

Ex. The equation $x^n(x-1)^n = 0$ has all its roots real; therefore $f^n(x) = 0$, or (Art. 26) since

$$f(x) = x^{2n} - nx^{2n-1} + \text{\&c.},$$

$$x^n - n \cdot \frac{n}{2n} x^{n-1} + \frac{n(n-1)}{1 \cdot 2} \frac{n(n-1)}{2n(2n-1)} x^{n-2} - \text{\&c.} = 0,$$

has n real roots, lying between 0 and 1.

54. If we know all the real roots of $f'(x) = 0$, and substitute them, in order, in $f(x)$, we may find how many real roots the proposed equation contains.

For let $\alpha, \beta, \gamma, \ldots \lambda$ be the roots of $f'(x) = 0$, arranged in order of magnitude, and let

$$\infty, \ \alpha, \ \beta, \ \gamma, \ldots \lambda, \ -\infty$$

be substituted for x in $f(x)$, giving results

$$+, f(\alpha), f(\beta), \ldots f(\lambda), \ \pm;$$

then there can only be one root greater than α, and one less than λ; for if there could be more, $f'(x) = 0$ would have a root situated between them, that is, a root $> \alpha$ or $< \lambda$, which is impossible, for $\alpha, \beta, \gamma, \ldots \lambda$ are all the real roots of $f'(x) = 0$ taken in order; also the other roots are situated singly between α and β, β and γ, &c. Hence if $f(\alpha)$ be positive, there is no root greater than α; for if there were two, these would include no root of $f'(x) = 0$, which is impossible; if negative, there is one root greater than α, and only one, for there cannot be three $> \alpha$, for the same reason as before; if $f(\beta)$ have the same sign as $f(\alpha)$ there is no root between α and β, otherwise there is one root, and so on: and if $f(\lambda)$ be positive for an equation of odd dimensions, or negative for one of even dimensions, there will be one root $< \lambda$, otherwise none.

It follows, therefore, that the number of real roots of $f(x) = 0$, will be exactly equal to the number of changes of sign in the results of the substitution of $\infty, \alpha, \beta, \gamma, \ldots \lambda, -\infty$ for x; and can be exactly determined whenever we can obtain a solution of $f'(x) = 0$.

Ex. 1. To determine whether $x^3 - qx + r = 0$ has all its roots possible.

The limiting equation is $3x^2 - q = 0$;

$$\therefore \ \alpha = \sqrt{\frac{q}{3}}, \ \beta = -\sqrt{\frac{q}{3}};$$

but $f(x) = x(x^2 - q) + r$, and for both substitutions

$$x^2 - q = -\frac{2q}{3};$$

$$\therefore \ f(\alpha) = \sqrt{\frac{q}{3}}\left(-\frac{2q}{3}\right) + r = -2\left(\frac{q}{3}\right)^{\frac{3}{2}} + r,$$

$$f(\beta) = -\sqrt{\frac{q}{3}}\left(-\frac{2q}{3}\right) + r = 2\left(\frac{q}{3}\right)^{\frac{3}{2}} + r.$$

If then $\left(\frac{r}{2}\right)^2 < \left(\frac{q}{3}\right)^3$, $f(\alpha)$ is negative; therefore there is one root $> \alpha$; also $f(\beta)$ is positive, therefore there is one root between α and β, and another less than β.

If $\left(\frac{r}{2}\right)^2 > \left(\frac{q}{3}\right)^3$, $f(\alpha)$ is positive; therefore there is no root greater than α, nor one between α and β, because $f(\beta)$ is positive; but there is one root $< \beta$, that is, one negative root which is the only real root.

If $\sqrt{q}$ be written for x, the result is $+r$; hence when all the roots are real, the greatest lies between $\sqrt{q}$ and $\sqrt{\frac{q}{3}}$.

These results were obtained by a different method (p. 45).

Ex. 2. $x^n - nqx + (n-1)r = 0$.

$\therefore f'(x) = nx^{n-1} - nq = 0$, which has one real root α and $n-2$ imaginary ones, or two real roots α and β and $n-3$ imaginary ones, according as n is even or odd (p. 19).

In the former case,

$$f(\alpha) = q^{\frac{1}{n-1}}(q - nq) + (n-1)r = (n-1)\left(-q^{\frac{n}{n-1}} + r\right),$$

which is negative or positive, according as $q^n >$ or $< r^{n-1}$; therefore the proposed equation, which has necessarily $n-2$ imaginary roots, will have two real roots or none, according as

$$q^n > \text{ or } < r^{n-1}.$$

In the latter case,

$$f(\alpha) = (n-1)\left(-q^{\frac{n}{n-1}} + r\right),\ f(\beta) = (n-1)\left(q^{\frac{n}{n-1}} + r\right),$$

which have different or the same signs, according as

$$q^n > \text{ or } < r^{n-1};$$

therefore the proposed equation (which has necessarily $n-3$ imaginary roots) will have three real roots, or one, according as

$$q^n > \text{ or } < r^{n-1}.$$

DES CARTES'S RULE OF SIGNS.

55. No equation, complete or incomplete, can have more positive roots than it has changes of signs from + to − and from − to +; and no complete equation can have more negative roots than it has continuations of the same sign.

Suppose the product of the factors corresponding to the imaginary and negative roots of an equation to be already formed; then we shall obtain the first member of the equation by multiplying this product by the factors $x-a$, $x-b$, &c. corresponding to the positive roots; and if we can shew that if any polynomial, whatever be the signs of its terms, be multiplied by $x-a$, the resulting polynomial will present at least one more change of signs than the original, the proposition will be established as far as regards the positive roots. Let the signs of any polynomial be

$$+ - + + - - - - + - +$$

and let it be multiplied by a factor $x-a$; then, writing down only the signs of the operation, we have

$$\begin{array}{l} + - + + - - - - + - + \\ \quad - + - - + + + + - + - \\ \hline \end{array}$$

$$\text{and } + - + \pm - \mp \mp \mp + - + -$$

for the signs of the result, the doubtful sign $\pm$ being written where the addition of unlike signs in the partial products is to be performed.

Upon comparing this result with the original polynomial, we observe that

(1) For every group of continuations there is a corresponding group of the same number of ambiguities.

(2) The two signs, preceding and succeeding each group of ambiguities, are contrary.

(3) There is a final sign superadded, contrary to that of the last term of the original polynomial.

Hence, in the most unfavourable case for changes, in which all the ambiguities become of the same sign, by (2) we may take the upper signs; therefore the signs of the result, excepting the last, are the same as in the original polynomial, or no change of signs is lost; and by (3) one more is introduced. Consequently, one change of signs at least is added, corresponding to each of the factors $x-a$, $x-b$, &c., and none ever lost; and therefore no equation, complete or incomplete, can have more positive roots than it has changes of sign.

To prove the second part of the proposition, change x into $-y$; then if the equation be complete, the continuations will be replaced by changes, and *vice versâ;* and by the preceding proof the transformed equation cannot have more positive roots than it has changes; and therefore the proposed cannot have a greater number of negative roots than it has continuations of sign.

Obs. This is *Des Cartes's* rule of signs, and it is applicable, as we see, to discover a limit to the number of positive roots of every equation; but not to discover a limit to the number of negative roots, unless the equation be complete, or unless we supply the deficient powers of x, each of which we may consider as having ± 0 for its coefficient. But for the negative roots, the best practical way, is to write $-y$ for x, and to find the limit to the number of positive roots of the transformed equation; and the theorem might be enuntiated thus; The equation $f(x)=0$ cannot have more positive roots than $f(x)$ has changes of sign, nor more negative roots than $f(-x)$ has changes of sign.

56. When an equation is complete, since to each term reckoning from the second corresponds either a change or a continuation of signs, the sum of the numbers expressing the changes and continuations is exactly equal to the degree of the equation.

Hence, when a complete equation has all its roots real, the number of changes is exactly equal to the number of positive roots, and the number of continuations to the number of negative roots. For if m, r, be respectively the number of positive and negative roots, and m', r', the number of changes and continuations $m + r = m' + r'$, each of these being equal to the degree of the equation; and as m cannot exceed m', nor r exceed r', the only way in which this equation can exist is $m = m'$, $r = r'$.

57. In incomplete equations, the above theorem will often enable us to detect the presence of imaginary roots.

Ex. 1. $x^3 + qx + r = 0$. This equation has visibly (supposing q and r essentially positive) no positive root, and one negative root (Art. 10); if we complete it, it becomes

$$x^3 \pm 0x^2 + qx + r = 0;$$

and taking the lower sign there is only one continuation of signs, and consequently only one negative root, which is therefore the only real root of the equation.

Ex. 2. $x^5 - 2x^2 + 1 = 0$. A limit of the number of positive roots is 2; and writing $-y$ for x, we get $y^5 + 2y^2 - 1 = 0$, a limit of the number of positive roots of which is 1, or the number of negative values of x cannot exceed 1; therefore the equation has at least two imaginary roots.

Ex. 3. $x^{12} + 5x^9 - 3x^8 + 4x^7 + 10x^5 - 4x^3 - 8x^2 + 5 = 0$ has at least four imaginary roots.

58. Every equation, which, otherwise complete, wants t consecutive terms, has at least t impossible roots, if t be even; and if t be odd, it has at least $t + 1$, or $t - 1$ impossible roots, according as the deficient group is between two terms of the same, or of contrary, signs.

Let the equation be

$$x^n + p_1 x^{n-1} + \dots + Px^{r+t+1} + Qx^r + \dots + p_{n-1}x + p_n = 0,$$

where P and Q have the same sign; then writing that sign before all the intermediate evanescent terms, let s = number

of changes and $n-s$ = number of continuations presented by the equation, which are limits, respectively, of the number of positive and negative roots. Now make the signs of all the intermediate evanescent terms alternately positive and negative, so that $t+1$ or t fresh changes may be introduced according as t is odd or even; then $n-s-t-1$ and $n-s-t$ are limits of the number of negative roots. Hence there cannot be more than s positive roots, and $n-s-t-1$ or $n-s-t$ negative roots, or more than $n-t-1$ or $n-t$ possible roots; and therefore there are at least $t+1$ or t impossible roots according as t is odd or even. Similarly, if t terms are wanting between two terms of different signs, it may be shewn that there are at least $t-1$ or t impossible roots, according as t is odd or even.

If $t=1$, or if only one term be wanting between two terms of the same sign, then the equation has at least two impossible roots; but if a term be wanting between two terms of contrary signs, we cannot in this way conclude anything respecting the nature of its roots.

Generally, in an incomplete equation, if the deficient terms be replaced by cyphers, and first be taken with such signs as to make the total number of changes the least possible, and $=s$; and secondly be taken with such signs as to make the total number of continuations the least possible, and $=t$; then the number of positive roots cannot exceed s, nor the number of negative roots, t; and the number of impossible roots is not less than $n-s-t$.

PROB. To shew that the equation

$$(x-a)(x-b)(x-c)-a'^2(x-a)-b'^2(x-b)-c'^2(x-c)=2a'b'c',$$

has for a limiting equation the quadratic to which it is reduced by making any two of the quantities a', b', c', vanish; and thence that all its roots are real.

Write the equation under the form

$$(x-c)\{(x-a)(x-b)-c'^2\}-$$
$$\{a'^2(x-a)+b'^2(x-b)+2a'b'c'\}=0,$$

and let α and β be the roots, taken in order, of

$$(x-a)\times(x-b)-c'^2=0,$$

the depressed equation when $a'=b'=0$; then α is greater than both a and b, and β less, as will appear by solving the equation. Hence, substituting $+\infty$, α, β, $-\infty$, for x in the proposed equation, the results are

$$+,\ -\{a'\sqrt{\alpha-a}\pm b'\sqrt{\alpha-b}\}^2,\ +\{a'\sqrt{a-\beta}\pm b'\sqrt{b-\beta}\}^2,\ -;$$

therefore there are three real roots; one $>\alpha$, another between α and β, and a third $<\beta$.

SECTION IV.

ON THE DEPRESSION OF EQUATIONS SOME OF WHOSE ROOTS HAVE PARTICULAR RELATIONS TO EACH OTHER, OR ARE OF A PARTICULAR FORM.

EQUAL ROOTS.

59. AMONG the cases in which an equation may be depressed by reason of particular relations existing among its roots, the most important is that where the polynomial which forms its first member has equal factors, or where the equation has equal roots; because, both in the method of determining the number and situation of the real roots of an equation, and also in that of approximating to the values of its incommensurable roots, one condition either essential or advantageous is, that the roots should be all different from one another, i. e. that the equation should contain no equal roots. We must therefore shew how we may be assured that a proposed equation has no equal roots; and when it has equal roots, we must shew how they may be found, and, consequently, the complete solution of the equation made to depend upon that of one or several equations having only unequal roots.

60. If the polynomial $f(x)$ and its derived function of the first order $f'(x)$ have no common measure, the equation $f(x) = 0$ has no equal roots; but if they have a common measure, the equation has equal roots, every simple factor of the common measure occurring one more time in $f(x)$ than it does in the common measure.

Let $a, b, c, \ldots l$ be all the roots real or imaginary of $f(x) = 0$; then, changing x into $y+h$, we have

$$f(y+h) = (y+h-a)(y+h-b)\ldots(y+h-l);$$

now if each member be expanded and arranged according to powers of y, the coefficient of y in the first member is $f'(h)$ (Art. 26), and in the second member it is

$$(h-b)(h-c)\ldots(h-l)+(h-a)(h-c)\ldots(h-l)$$
$$+(h-a)(h-b)\ldots(h-l)+\&c.,$$

each of the factors $h-a$, $h-b$, &c., being left out in succession; therefore, equating these coefficients and replacing h by x, we get

$$f'(x) = (x-b)(x-c)\ldots(x-l)+(x-a)(x-c)\ldots(x-l)$$
$$+(x-a)(x-b)\ldots(x-l)+\&c.$$

Hence, if $f(x)$ have only one factor $= x-a$, $f'(x)$ is not divisible by $x-a$, because one of its terms does not involve $x-a$; and in the same manner it may be proved that any other of the unequal factors of $f(x)$ is not a divisor of $f'(x)$. Therefore, if $f(x)$ be composed of unequal factors, $f(x)$ and $f'(x)$ have no common measure.

Again, $f'(x) = (x-a)(x-b)(x-c)\ldots(x-l)\times$

$$\left\{\frac{1}{x-a}+\frac{1}{x-b}+\frac{1}{x-c}+\ldots+\frac{1}{x-l}\right\}.$$

Now suppose the equation $f(x) = 0$ to have m roots equal to a, r roots equal to b, p roots equal to c,

$$\therefore f'(x) = (x-a)^m(x-b)^r(x-c)^p\ldots(x-l)\times$$
$$\left\{\frac{m}{x-a}+\frac{r}{x-b}+\frac{p}{x-c}+\ldots+\frac{1}{x-l}\right\}.$$

Therefore $f'(x)$ is divisible by

$$(x-a)^{m-1}(x-b)^{r-1}\times(x-c)^{p-1};$$

and therefore, if $f(x)$ has equal factors, $f(x)$ and $f'(x)$ have a common measure, formed by the product of all those factors, each raised to a power less by unity than that to which it is raised in $f(x)$.

Ex. 1. $$f(x) = x^3 - 3x^2 - 9x + 27 = 0,$$
$$f'(x) = 3x^2 - 6x - 9;$$
the greatest common measure of $f(x)$ and $f'(x)$ will be found to be $x-3$; therefore the proposed equation has two roots equal to 3.

Ex. 2. $x^6 - 2x^5 - 4x^4 + 12x^3 - 3x^2 - 18x + 18 = 0$;
it is the same as $(x^2-3)^2(x^2-2x+2) = 0$.

61. Hence, if we know the value of one of the equal roots of an equation, we may find its multiplicity, that is, the number of times it is repeated, by substituting it in the derived functions taken in order; then the degree of the first of the derived functions which does not vanish by the substitution, expresses the multiplicity of the root.

For suppose the factor $x-a$ to be repeated m times,
$$\therefore f(x) = (x-a)^m . \phi(x),$$
where $\phi(x)$ has no factor $= x-a$.

Change x into $a+h$, then (Art. 27)
$$h^m . \phi(a+h) = f(a) + f'(a)\frac{h}{1} + f''(a)\frac{h^2}{1.2} + \ldots$$
$$+ f^m(a)\frac{h^m}{\lfloor m} + \ldots + h^n.$$

Now the first member is divisible by h^m, but by no higher power of h; therefore the second member is so, and therefore we must have
$$f'(a) = 0, \ f''(a) = 0, \ \&c., \ f^{m-1}(a) = 0;$$
but $f^m(a)$ will be a finite quantity, because the coefficient of h^m is so in the first member; that is, the first of the derived functions which does not vanish for $x = a$, is that whose order is m, the number of times the root a is repeated.

Ex. $x^5 + 2x^4 - 6x^3 - 4x^2 + 13x - 6 = 0$; to find how often the root unity is repeated.

It will be found that $f'''(x)$ is the first derived function which does not vanish, when $x = 1$; therefore the root 1 is repeated three times.

62. To decompose a polynomial having equal factors, into other polynomials which have only unequal factors.

Let $$f(x) = X_1 X_2^2 X_3^3 \dots X_m^m,$$
where X_1 denotes the product of the factors which enter only once, X_2 the product of those which enter twice, &c., and X_m the product of those which enter m times; then if $f_1(x)$ denote the greatest common measure of $f(x)$ and $f'(x)$,
$$f_1(x) = X_2 X_3^2 X_4^3 \dots X_m^{m-1}.$$

Again, treating the polynomial $f_1(x)$ in the same manner as $f(x)$ was treated, if $f_2(x)$ denote the greatest common measure of $f_1(x)$ and $f_1'(x)$,
$$f_2(x) = X_3 X_4^2 \dots X_m^{m-2};$$
and proceeding in this manner, we shall at last come to
$$f_{m-1}(x) = X_m;$$
beyond which, if the process be continued, we find $f_m(x) = 1$, as X_m has only unequal factors. Hence, by division, we obtain
$$\frac{f(x)}{f_1(x)} = X_1 X_2 X_3 \dots X_m = \phi_1(x) \text{ suppose},$$
$$\frac{f_1(x)}{f_2(x)} = X_2 X_3 \dots\dots X_m = \phi_2(x),$$
$$\frac{f_2(x)}{f_3(x)} = X_3 X_4 \dots\dots X_m = \phi_3(x),$$
$$\dots = \dots\dots\dots\dots\dots = \dots$$
$$\frac{f_{m-2}(x)}{f_{m-1}(x)} = X_{m-1} X_m = \phi_{m-1}(x),$$
$$\frac{f_{m-1}(x)}{f_m(x)} = X_m = \phi_m(x).$$

Hence $$\frac{\phi_1(x)}{\phi_2(x)} = X_1, \ \frac{\phi_2(x)}{\phi_3(x)} = X_2, \dots = \dots$$
$$\frac{\phi_{m-1}(x)}{\phi_m(x)} = X_{m-1}, \ \phi_m(x) = X_m.$$

The solution of the original equation is thus reduced to that of the equations

$$X_1 = 0, \quad X_2 = 0, \ \ldots \ X_m = 0,$$

each of which contains only unequal roots.

63. Hence the process of decomposing a polynomial $f(x)$ that has equal factors, may be thus represented;

$$\begin{array}{lll} f(x) & f_1(x) \ldots f_{m-1}(x) & f_m(x) \\ \phi_1(x) & \phi_2(x) \ldots \phi_m(x) & \\ X_1 & X_2 \ \ldots X_m. & \end{array}$$

In the first line, each term, beginning with $f_1(x)$, is the greatest common measure of the preceding term and its derived function, and the last term $f_m(x)$ is unity; in the second line, each term is the quotient of the division of that term of the first line under which it stands by the following term; and in the third line, each term is the quotient of the division of that term of the second line under which it stands by the following term, and any term may equal unity. Then each of the functions $X_1, X_2, \ldots X_m$, will, by its subscribed index, shew the multiplicity of the factors of which it is composed, in the original polynomial; and, by its degree, the number of factors that have that multiplicity; and if any one of them X_r equals unity, then $f(x)$ admits no factor occurring r times.

Ex. 1. $f(x) = x^8 - 7x^7 - 2x^6 + 118x^5 - 259x^4 - 83x^3 + 612x^2 - 108x - 432,$

$$f_1(x) = x^4 - 7x^3 + 13x^2 + 3x - 18,$$
$$f_2(x) = x - 3,$$
$$f_3(x) = 1,$$
$$\phi_1(x) = x^4 - 15x^2 + 10x + 24,$$
$$\phi_2(x) = x^3 - 4x^2 + x + 6,$$
$$\phi_3(x) = x - 3,$$
$$X_1 = x + 4,$$
$$X_2 = x^2 - x - 2,$$
$$X_3 = x - 3,$$
$$\therefore f(x) = (x+4)(x^2 - x - 2)^2 (x-3)^3.$$

Ex. 2.

$x^8 - 12x^7 + 53x^6 - 92x^5 - 9x^4 + 212x^3 - 153x^2 - 108x + 108 = 0$;
it is the same as

$$(x-1)(x-2)^2(x+1)^2(x-3)^3 = 0.$$

Ex. 3. $x^n - nqx + (n-1)r = 0$ will have a pair of equal roots, if $q^n = r^{n-1}$.

The limiting equation is $nx^{n-1} - nq = 0$; $\therefore x = q^{\frac{1}{n-1}}$ is the value of the equal roots, if the equation admits any; substituting it in the proposed, we find

$$(q - nq)\,q^{\frac{1}{n-1}} + (n-1)\,r = 0 \dots\dots\dots (1),$$
$$\text{or } q^n = r^{n-1},$$

for the relation among the coefficients, in order that the proposed may admit a pair of equal roots. Moreover, when n is even, r must be positive, and the root which recurs is $q^{\frac{1}{n-1}}$; when n is odd, r may be either positive or negative, but in the former case the root which recurs is $+q^{\frac{1}{n-1}}$. and in the latter case $-q^{\frac{1}{n-1}}$, as appears from (1).

COMMENSURABLE ROOTS.

64. Commensurable roots are those whose exact values can be expressed by finite numbers either whole or fractional, and therefore of course not involving in their expressions any irrational quantity. When the coefficients are whole numbers, and that of the first term unity, the commensurable roots are necessarily whole numbers, as will be proved; in other cases they may be fractions; but in all cases they can be readily obtained, and the equation depressed.

An equation is said to be *irreducible* when, its coefficients being given numbers, its first member admits of no commensurable factor, that is, one whose coefficients have exact numerical values.

65. If in any equation the coefficient of the highest power of the unknown quantity be unity, and the other coefficients be whole numbers, the equation can have only whole numbers for its commensurable roots.

If possible, let $\frac{a}{b}$, a fraction in its lowest terms, be a commensurable root of the equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \dots + p_n = 0,$$

$$\text{then} \left(\frac{a}{b}\right)^n + p_1 \left(\frac{a}{b}\right)^{n-1} + p_2 \left(\frac{a}{b}\right)^{n-2} + \dots + p_n = 0;$$

therefore, multiplying by b^{n-1} and transposing,

$$-\frac{a^n}{b} = p_1 a^{n-1} + p_2 a^{n-2} b + \dots + p_n b^{n-1};$$

that is, a fraction in its lowest terms is equal to a whole number, which is impossible; therefore $\frac{a}{b}$ is not a root of the equation. If therefore the equation can be satisfied by real quantities, since they are not expressible in the form of a vulgar fraction, they must be either whole numbers or interminable decimals. Hence the commensurable roots can only be whole numbers; and the other real roots are incommensurable; that is, they cannot be expressed by finite rational numbers, either whole or fractional, and therefore can never be exactly known; but their values may be approximated to with any degree of accuracy, as will be shewn.

METHOD OF DIVISORS.

66. The commensurable roots of $f(x) = 0$, which are necessarily whole numbers, may be always found by the following process, called the Method of Divisors, proposed by *Newton*.

Suppose a to be an integral root; then, substituting a for x, and reversing the order of the terms, we have

$$p_n + p_{n-1} a + p_{n-2} a^2 + \dots + p_1 a^{n-1} + a^n = 0;$$

$$\therefore \frac{p_n}{a} + p_{n-1} + p_{n-2}a + \ldots + p_1 a^{n-3} + a^{n-1} = 0.$$

Hence $\frac{p_n}{a}$ is an integer which we may denote by q_1; substituting, and dividing again by a, we get

$$\frac{q_1 + p_{n-1}}{a} + p_{n-2} + \ldots + p_1 a^{n-3} + a^{n-2} = 0.$$

Similarly, $\frac{q_1 + p_{n-1}}{a}$ is an integer $= q_2$ suppose; and proceeding in this manner, we shall at last arrive at

$$\frac{q_{n-1} + p_1}{a} + 1 = 0.$$

Hence, that a may be a root of the equation, the last term p_n must be divisible by it, so must the sum of the quotient and next coefficient, $q_1 + p_{n-1}$; and continuing the uniform operation, the sum of each coefficient and the preceding quotient must be divisible by a, the final result being always -1.

If therefore we take the quotients of the division of the last term by each of the divisors of the last term which are comprised within the limits of the roots, and add these quotients to the coefficient of the last term but one; divide these sums, some of which may be equal to zero, by the respective divisors, add the new quotients which are integers or zero (neglecting the others) to the next coefficient and divide by the respective divisors; and so on through all the coefficients (dropping every divisor as soon as it gives a fractional quotient), those divisors of the last term which give -1 for a final result are the integral roots of the equation; and we shall thus obtain all the integral roots, unless the equation have equal roots, the test of which will be that some of the roots already found, satisfy $f'(x) = 0$; and the number of times that any one is repeated will be expressed by the degree of derivation of the first of the derived functions which that root does not reduce to zero, when

written in it for x (Art. 61). It is best to ascertain by direct substitution whether $+1$ and -1 are roots, and so to exclude them from the divisors to be tried.

Ex. 1. $$x^3 + 3x^2 - 8x + 10 = 0.$$

Here the roots lie between $\frac{8}{4} + 1$ and -11 (Arts. 44, 42), and the divisors of the last term are $\pm \{2, 5, 10\}$,

$$\begin{array}{rcccc} \therefore\ a = & 2 & -2 & -5 & -10 \\ q_1 = & 5 & -5 & -2 & -1 \\ q_1 + (-8) = & -3 & -13 & -10 & -9 \\ q_2 = & \times & \times & 2 & \times \\ q_2 + 3 = & & & 5 & \\ q_3 = & & & -1. & \end{array}$$

Therefore -5 is the only commensurable root; and it is not repeated since it does not satisfy the equation

$$f'(x) = 3x^2 + 6x - 8 = 0.$$

Ex. 2. $$x^5 - 5x^4 + x^3 + 16x^2 - 20x + 16 = 0.$$

Here limits of the roots are 6 and -4; and the commensurable roots are 4, 2, -2.

Ex. 3. $x^4 + 5x^3 - 2x^2 - 6x + 20 = 0$; $x = -2$, or -5.

67. The number of divisors to be tried may be lessened by observing, that if the roots of $f(x) = 0$ were diminished by any whole number m, the last term of the transformed equation $f(y + m) = 0$ would be $f(m)$; if therefore a were an integral value of x, $a - m$ would be an integral value of y, and would be therefore a divisor of $f(m)$. Hence any divisor, a, of the last term of $f(x)$ is to be rejected which does not satisfy the condition $\frac{f(m)}{a - m} =$ an integer, when for m any integer, such as ± 1, ± 10, &c., is substituted.

Ex. 1. $$x^3 - 5x^2 - 18x + 72 = 0.$$

Changing the signs of the alternate terms, we have

$$x^3 + 5x^2 - 18x - 72 = 0, \text{ or } x^3 - 72 + 5x\left(x - \frac{18}{5}\right) = 0;$$

therefore the roots lie between 19 and -5.

But $\quad f(1) = 50, \; f(-1) = 84, \; f(-3) = 54;$
and the only admissible divisors of 72, which, when diminished by 1, divide 50, are

$$6, 3, 2, -4;$$

also, all these divisors, when increased by 1, divide 84; but only 6, 3, -4, when increased by 3, divide 54;

$$\therefore \; 6, 3, -4,$$

are the only divisors which need to be tried; and they will all be found to be roots.

Ex. 2. $\quad x^3 - 6x^2 + 169x - (42)^2 = 0. \quad x = 9.$

68. If a proposed equation have fractional coefficients, or if its first term be affected with a coefficient, since (Art. 30) it can be transformed into another equation with first term unity and every coefficient a whole number, this method will enable us to find the commensurable roots of every equation under a rational form. If the coefficients be whole numbers and the first term be p_0x^n, and we only wish to find the roots which are integers, no transformation will be necessary; only every divisor of the last term which is a root, will lead to a result $-p_0$ instead of -1.

Ex. $\qquad 6x^4 - 25x^3 + 26x^2 + 4x - 8 = 0.$

It is the same as

$$(x-2)^2(3x-2)(2x+1) = 0.$$

SOLUTION OF RECIPROCAL EQUATIONS.

69. These are equations which are not altered by changing x into $\frac{1}{x}$, and of which the roots are consequently

of the form a, $\frac{1}{a}$, b, $\frac{1}{b}$, &c., together with $+1$ or -1 several times repeated. The particular form of the equation necessary to satisfy this condition, investigated at Art. 33, is such as to permit a great simplification in its solution; when the degree does not exceed the ninth, the solution can be completely effected.

In Art. 34 it is proved that every reciprocal equation of an odd order will have $x+1$ or $x-1$ for a factor, according as its last term is positive or negative; and that every reciprocal equation of an even order with its last term negative (and consequently having no middle term) will have x^2-1 for a factor; and that if these factors be expelled, the depressed equation, in both cases, will be a reciprocal equation of an even order with its last term positive; which may therefore be taken as the standard form of reciprocal equations.

70. The roots of a reciprocal equation of an even number of dimensions exceeding a quadratic, may be found by the solution of an equation of half the number of dimensions.

Let the equation be

$$x^{2n}+px^{2n-1}+qx^{2n-2}+\ldots+kx^{n+1}+lx^n+kx^{n-1}+\ldots$$
$$\ldots+qx^2+px+1=0;$$

then, collecting the terms which are equidistant from the extremities in pairs, and dividing by x^n, we have

$$x^n+\frac{1}{x^n}+p\left(x^{n-1}+\frac{1}{x^{n-1}}\right)+\ldots+k\left(x+\frac{1}{x}\right)+l=0.$$

Let $x+\frac{1}{x}=y$, then because

$$x^m+\frac{1}{x^m}=y\left(x^{m-1}+\frac{1}{x^{m-1}}\right)-\left(x^{m-2}+\frac{1}{x^{m-2}}\right),$$

making $m=2, 3\ldots n$, successively, and substituting in each equation from the preceding, we get

$$x^2 + \frac{1}{x^2} = y^2 - 2,$$

$$x^3 + \frac{1}{x^3} = y(y^2 - 2) - y = y^3 - 3y,$$

$$x^4 + \frac{1}{x^4} = y(y^3 - 3y) - (y^2 - 2) = y^4 - 4y^2 + 2,$$

$$\ldots\ldots = \ldots\ldots\ldots\ldots\ldots\ldots = \ldots\ldots\ldots\ldots$$

$$x^n + \frac{1}{x^n} = y^n - ny^{n-2} + \frac{n(n-3)}{1.2} y^{n-4} - \&c.$$

Hence, by substitution, the original equation will be transformed into an equation of n dimensions in y; any root of which, a, will give two roots of the original equation, by means of the relation $x + \frac{1}{x} = a$; and a quadratic factor, $x^2 - ax + 1$. The general term of the series for $x^n + \frac{1}{x^n}$ is given in Ex. 3, Art. 154.

We may remark in passing that any one of the above polynomials in y, put equal to zero, would furnish an equation having all its roots real and unequal, and situated between -2 and $+2$; for $2 \cos n\theta = x^n + \frac{1}{x^n} = 0$, is satisfied by n different real values of $2 \cos \theta = x + \frac{1}{x}$, (p. 29).

Ex. 1.

$$x^9 + x^8 - 9x^7 + 3x^6 - 8x^5 - 8x^4 + 3x^3 - 9x^2 + x + 1 = 0.$$

Expelling the root -1, by means of Art. 6, we get for the depressed equation

$$x^8 + (-1+1)x^7 + (0-9)x^6 + (9+3)x^5 + (-12-8)x^4$$
$$+ (20-8)x^3 + (-12+3)x^2 + (9-9)x + 1 = 0,$$

$$\text{or } x^4 + \frac{1}{x^4} - 9\left(x^2 + \frac{1}{x^2}\right) + 12\left(x + \frac{1}{x}\right) - 20 = 0;$$

$$\therefore\ y^4 - 4y^2 + 2 - 9(y^2 - 2) + 12y - 20 = 0,$$

$$\text{or } y^4 - 13y^2 + 12y = 0;$$

$$\therefore\ y = 0,\ y = 1; \text{ and the other roots are } 3, -4;$$

therefore the proposed equation is resolved into

$$(x+1)(x^2+1)(x^2-x+1)(x^2-3x+1)(x^2+4x+1) = 0.$$

Ex. 2. $\qquad 2x^6 - 5x^5 + 4x^4 - 4x^2 + 5x - 2 = 0.$

Expelling the factor $x^2 - 1$, the depressed equation is

$$2x^4 - 5x^3 + 6x^2 - 5x + 2 = 0,$$

which may be resolved into

$$(x-1)^2(2x^2 - x + 2) = 0.$$

It may be observed that, by precisely the same process, the equation

$$x^{2n} + px^{2n-1} + \ldots + kx^{n+1} + lx^n + kmx^{n-1} + hm^2x^{n-2} + \ldots$$
$$\ldots + pm^{n-1}x + m^n = 0,$$

admits of the same reduction as the recurring equation which it becomes when $m = 1$; the formulæ to be used being

$$x + \frac{m}{x} = y,\ x^{n+1} + \frac{m^{n+1}}{x^{n+1}} = y\left(x^n + \frac{m^n}{x^n}\right) - m\left(x^{n-1} + \frac{m^{n-1}}{x^{n-1}}\right).$$

71. The following are other instances in which equations are solvable, on account of their roots being known to have particular relations to one another.

Ex. 1. $\qquad x^4 - \frac{85}{4}x^3 + \frac{357}{4}x^2 - 85x + 16 = 0,$

roots in geometrical progression.

They are therefore of the forms $\frac{a}{r^3}$, $\frac{a}{r}$, ar, ar^3;

$$\therefore \text{(Art. 19) } a^4 = 16 \text{ or } a = 2.$$

$$\text{Also } \frac{357}{4} = \frac{a^2}{r^4} + \frac{a^2}{r^2} + a^2 + a^2 + a^2r^2 + a^2r^4;$$

$$\therefore \frac{357}{16} = \left(r^2 + \frac{1}{r^2}\right)^2 + \left(r^2 + \frac{1}{r^2}\right), \text{ which gives } r = 2;$$

consequently the roots are $\frac{1}{4}$, 1, 4, 16.

Ex. 2. $x^n + p_1 x^{n-1} + p_2 x^{n-2} + \&c. = 0$, roots in arithmetical progression.

They are therefore of the forms a, $a + b$, $a + 2b$, &c.

$$\therefore -p_1 = \{2a + (n-1)b\}\frac{n}{2} = na + \frac{n(n-1)}{2}b,$$

$$p_1^2 - 2p_2 = a^2 + (a+b)^2 + \&c. = na^2 + \{1 + 2 + 3 + \ldots + (n-1)\}2ab$$
$$+ \{1^2 + 2^2 + \ldots + (n-1)^2\}b^2$$
$$= na^2 + n(n-1)ab + \frac{(2n-1)(n-1)n}{6}b^2;$$

subtracting the square of the former from the latter equation multiplied by n, we get b^2; and then a is known from the former, by substituting for b its value.

In general, the equation $f(x) = 0$ may be depressed, if it be reducible, and if we know a relation $b = \phi(a)$, between two of its roots, a and b.

Write $\phi(x)$ instead of x in $f(x)$, and let the resulting polynomial be $F(x)$; then $f(x)$ and $F(x)$ are both reduced to zero by making $x = a$; for a and b are roots of $f(x) = 0$ by supposition; and to write a for x in $F(x)$, is the same thing as to write b for x in $f(x)$; therefore $f(x)$ and $F(x)$ have a common measure $x - a$, which may be found; whence a, and $b = \phi(a)$, become known, and the equation may be depressed two dimensions.

Ex. $x^4 + 2x^3 - 9x^2 - 22x - 22 = 0$; the sum of two roots is -2. The roots are $-1 \pm \sqrt{-1}$ and $\pm\sqrt{11}$.

In depressing the equation $f(x) = 0$, two of whose roots are known to have the number h for their sum, by finding the greatest common divisor D of $f(x)$ and $f(h - x)$, D will

be of the second degree in x, only when there is but one pair of roots whose sum $= h$, and no root $= \frac{1}{2}h$; and D will be of higher dimensions when there are several ways of taking two roots whose sum is h. The method becomes illusory when all the roots can be distributed in pairs whose sum is h. Thus suppose

$$f(x) = (x-1)(x-2)(x-4)(x-5),$$

$$\text{then } f(6-x) = (x-5)(x-4)(x-2)(x-1),$$

which is identical with the proposed. But in this case we get for each pair of factors where $a + b = h$,

$$(x-a)(x-b) = (x-\tfrac{1}{2}h)^2 - \tfrac{1}{4}(a-b)^2;$$

so that, if we put $x - \frac{1}{2}h = \sqrt{z}$, the equation is reduced to $\frac{1}{2}n$ dimensions in z. This branch of the subject will be resumed at Art. 161.

ALGEBRAICAL SOLUTION OF BINOMIAL EQUATIONS

72. These are equations of the form $x^n \pm a = 0$, containing only a single power of the unknown quantity, which may be reduced to reciprocal equations; for let α be the arithmetical value of $\sqrt[n]{a}$, and for x write αx, then the equation becomes $x^n \pm 1 = 0$, which is reciprocal.

Although we have already obtained the complete solution of this equation (p. 18), so that with the aid of a Table of Sines, the numerical values of the roots may be easily found in the form $a + b\sqrt{-1}$, as approximately as can be desired; yet the solution by a purely algebraical process deserves attention, since in it additional properties of the roots are brought to light; and these roots, that is, the n^{th} roots of unity or of negative unity, are indispensable in the Algebraical solution of Equations, and are not unfrequently employed in several of the higher branches of Analysis.

73. In all cases of the equation $x^n \pm 1 = 0$, having expelled the real factors if there be any, if we transform it

by the substitution $y = x + \frac{1}{x}$, so that $x^2 - yx + 1 = 0$, since y will be the sum of a pair of conjugate roots, y will always be real, as every value of x is impossible, and equal to $2 \cos \phi$ where ϕ is some multiple of $\frac{1}{n}\pi$; and therefore the equation will be transformed into another of half the number of dimensions having all its roots real and situated between -2 and $+2$. The transformation may be readily effected thus: Taking the case $x^{2m+1} - 1 = 0$, and expelling the factor $x - 1$, and dividing by x^m, we get

$$x^m + \frac{1}{x^m} + x^{m-1} + \frac{1}{x^{m-1}} + \ldots + x + \frac{1}{x} + 1 = 0.$$

Calling the first member U_m, and putting

$$y = x + \frac{1}{x}, \quad V_m = x^m + \frac{1}{x^m}, \text{ we have}$$

$$V_m = y V_{m-1} - V_{m-2}, \text{ (Art. 70)},$$
$$V_{m-1} = y V_{m-2} - V_{m-3},$$
$$\ldots\ldots = \ldots\ldots$$
$$V_2 = y V_1 - 2.$$

Hence, adding these equations together, we get

$$U_m - y - 1 = y (U_{m-1} - 1) - U_{m-2} - 1,$$
$$\text{or } U_m = y V_{m-1} - U_{m-2}.$$

Hence, since $U_1 = y + 1, \quad U_2 = y^2 + y - 1,$

$$U_3 = y^3 + y^2 - 2y - 1,$$
$$U_4 = y^4 + y^3 - 3y^2 - 2y + 1,$$
$$\ldots = \ldots$$
$$U_m = y^m + y^{m-1} - (m-1) y^{m-2} - (m-2) y^{m-3}$$
$$+ \frac{(m-2)(m-3)}{1.2} y^{m-4} + \frac{(m-3)(m-4)}{1.2} y^{m-5} - \&c. = 0,$$

an equation whose roots are all real and unequal, and lying between -2 and 2. The general term of U_m may be deduced from that of V_m (Art. 70)*. This process readily furnishes the solution of all binomial equations as far as $x^{10} \pm 1 = 0$; but the solution of $x^{11} - 1 = 0$ by this method would require the solution of a complete equation of the fifth degree.

74. If α be an imaginary root of $x^n - 1 = 0$, then α^m will also be a root, m being any number positive or negative.

For since α is a root, $\alpha^n = 1$; therefore $(\alpha^n)^m = 1$,

$$\text{or } (\alpha^m)^n - 1 = 0; \text{ therefore } \alpha^m \text{ is a root.}$$

Also, if α be an imaginary root of $x^n + 1 = 0$, then α^m is also a root, m being any *odd* number positive or negative.

For $\alpha^n = -1$, $\therefore (\alpha^n)^m = (-1)^m = -1$, since m is odd,

$$\text{or } (\alpha^m)^n + 1 = 0; \ \therefore \alpha^m \text{ is a root.}$$

In both cases, all the roots are manifestly unequal (Art. 60), for the derived function nx^{n-1} can have no factor in common with $x^n \pm 1$.

75. The equations $x^n - 1 = 0$, and $x^m - 1 = 0$, can have no other common root, except unity, when m and n are prime to one another; and in other cases they have in common all the roots of $x^q - 1 = 0$, q being the greatest common measure of m and n.

For suppose, if possible, α to be another common root; and let a and b be two numbers determined so as to satisfy the equation $an - bm = 1$, which can always be done (Art. 143), since m and n are prime to one another; then $\alpha^n = 1$, $\alpha^m = 1$, $\alpha^{an} = 1$, $\alpha^{bm} = 1$; $\therefore$ by division we get $\alpha^{an-bm} = 1$, or $\alpha = 1$, which is consequently the only common root.

But if m and n be not prime to one another, then in seeking the greatest common divisor of $x^m - 1$ and $x^n - 1$, the

* This can best be effected by means of the relation

$$U_m = \frac{1}{m}\frac{dV_m}{dy} + \frac{1}{m+1}\frac{dV_{m+1}}{dy}$$

successive reductions effected upon the indices of x, will be the same as in the remainders met with in seeking the greatest common measure of m and n; if therefore q be that common measure, then $x^q - 1$ is the greatest common divisor of $x^m - 1$ and $x^n - 1$.

Hence when n is a prime number, the equation $x^n - 1 = 0$ has no root in common, except unity, with any equation of the same form and of an inferior degree.

76. The imaginary roots of $x^n - 1 = 0$, n being a prime number, are the same as the several powers of α from 1 to $n-1$, α being any one of the imaginary roots.

The quantities α, α^2, α^3, ... α^{n-1} are roots by what has been proved, and no two of them are equal; for, if possible, let $\alpha^p = \alpha^q$, p and q being both less than n, therefore $\alpha^{p-q} = 1$; or, α is a root of $x^{p-q} - 1 = 0$, and also of $x^n - 1 = 0$, which is impossible, because $p - q$ and n are prime to one another; therefore the roots of the equation are all contained in the series

$$1,\ \alpha,\ \alpha^2,\ \dots\ \alpha^{n-1};$$

and if it be continued, the roots recur in the same order, for

$$\alpha^n = 1,\ \ \alpha^{n+1} = \alpha^n . \alpha = \alpha,\ \ \alpha^{n+2} = \alpha^n . \alpha^2 = \alpha^2,\ \&c.$$

77. This property of producing all the other roots by its different powers, which, when n is prime, belongs to any one of the imaginary roots, is, in other cases, generally confined to the first imaginary root, α, determined by *De Moivre's* formula, (as proved, p. 21), or to its conjugate; or rather to any root α^m, provided m be prime to n, or to its conjugate. If therefore β be any root of $x^n - 1 = 0$, it is always true that any power of β is also a root; but not always true that all the roots can be produced by powers of β.

Thus, in the case $x^6 - 1 = 0$, or $(x^3 - 1)(x^3 + 1) = 0$, if we take $\beta = \frac{1}{2}(-1 + \sqrt{-3})$, we can, by its powers from 0 to 5, only produce the roots of $x^3 - 1 = 0$ twice over; but we can by the powers of α produce all the six roots, if we take

$$\alpha = \tfrac{1}{2}(1 + \sqrt{-3}) = \cos\frac{2\pi}{6} + \sqrt{-1}\,\sin\frac{2\pi}{}$$

Any root of $x^n - 1 = 0$ which does not belong to any equation of the same form and of an inferior degree, and whose powers consequently from 1 to $n-1$ have distinct values, is called a primitive root of $x^n - 1 = 0$. When n is a prime number, every root except unity is a primitive root. We proceed now to shew the existence of primitive roots for a binomial equation whose degree is a composite number, and to determine the number of them.

78. A primitive root of the equation $x^m = 1$, whose index m is the μ^{th} power of a prime number p, will $= \beta_1\beta_2\beta_3 \dots \beta_\mu$: where β_1 is a root, different from unity, of $x^p = 1$; β_2 any root of $x^p = \beta_1$; β_3 any root of $x^p = \beta_2$, &c.; and β_μ any root of $x^p = \beta_{\mu-1}$.

Every non-primitive root of $x^m = 1$ must belong to some equation $x^q = 1$ where q is a divisor of m; but every divisor of m, except itself, is a divisor of $p^{\mu-1}$; therefore the roots of $x^q = 1$, and consequently all the non-primitive roots of the proposed, are contained in $x^{p^{\mu-1}} = 1$; and it is evident that all the roots of this last equation belong to the proposed; therefore the number of the non-primitive roots of the proposed is $p^{\mu-1}$; and consequently the number of the primitive roots is $p^\mu - p^{\mu-1}$. To form these, let $\beta_1\beta_2\beta_3 \dots \beta_\mu$ denote, respectively, roots of the equations

$$x^p = 1,\ x^p = \beta_1,\ x^p = \beta_2,\ \dots\ x^p = \beta_{\mu-1},$$

and assume

$$\alpha = \beta_1\beta_2 \dots \beta_{\mu-1}\beta_\mu \dots\dots\dots\dots\dots (1);$$

then this formula will represent all the roots of the proposed. For since β_1 has p values, and to each of them correspond p values of β_2, and to each of the values of β_2 correspond p values of β_3, and so on, therefore the expression for α admits of p^μ values. And each of them is a root of the proposed; for

$$\beta_1^p = 1,\ \beta_2^{p^2} = 1,\ \beta_3^{p^3} = 1 \dots \beta_\mu^{p^\mu} = 1;$$

$$\therefore\ \alpha^{p^\mu} = 1.$$

And all the values of α are different from one another. For suppose two of them to be equal to one another, viz.

$$\beta_1\beta_2\beta_3 \ldots \beta_\mu = \beta'_1\beta'_2\beta'_3 \ldots \beta'_\mu \ldots\ldots\ldots\ldots (2),$$

then raising both sides to the power p, and observing that

$$\left.\begin{matrix} \beta_1^p = 1, & \beta_2^p = \beta_1 & \ldots & \beta_\mu^p = \beta_{\mu-1} \\ \beta'^p_1 = 1, & \beta'^p_2 = \beta'_1 & \ldots & \beta'^p_\mu = \beta'_{\mu-1} \end{matrix}\right\} \ldots\ldots\ldots (3),$$

we get

$$\beta_1\beta_2 \ldots \beta_{\mu-1} = \beta'_1\beta'_2 \ldots \beta'_{\mu-1} \ldots\ldots\ldots\ldots (4),$$

consequently from (2) we get $\beta_\mu = \beta'_\mu$.

If we repeat the same operation upon (4) that has been performed upon (2), we next find $\beta_{\mu-1} = \beta'_{\mu-1}$; and proceeding in this manner, we arrive at the conclusion that the equation (2) cannot subsist, unless all the factors on one side be respectively equal to those on the other; whence it follows that the assumed formula for α will furnish all the m roots. As the non-primitive roots satisfy $x^{p^{\mu-1}} = 1$, whenever the value of α given by (1) is a non-primitive root, we must have

$$(\beta_1\beta_2 \ldots \beta_{\mu-1}\beta_\mu)^{p^{\mu-1}} = 1,$$

or, suppressing the factors equal to unity,

$$\beta_\mu^{p^{\mu-1}} = 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5).$$

But from (3) we deduce

$$\beta_\mu^{p^{\mu-1}} = \beta_{\mu-1}^{p^{\mu-2}} = \ldots = \beta_2^p = \beta_1,$$

therefore equation (5) requires that we have $\beta_1 = 1$; consequently the value of α given by formula (1) will be a non-primitive root when $\beta_1 = 1$, and a primitive root in the contrary case. Hence the resolution of $x^n = 1$, whose degree is the μ^{th} power of a prime number p, is reduced to finding one root β_1 different from unity of $x^p = 1$; next any one root β_2 of $x^p = \beta_1$; then any one root β_3 of $x^p = \beta_2$; and so on, through μ equations of the p^{th} degree; for by that means we shall obtain a primitive root of the proposed equation, which by its powers will furnish all the other roots.

79. The solution of the general case, where the degree m of the equation $x^m = 1$ is any composite number, can be made to depend on the solution of equations of the same form, whose degrees are the prime numbers, or the powers of prime numbers, which are divisors of m.

Let $m = p^\mu q^\nu \ldots r^\lambda$, where $p, q \ldots r$ are distinct prime numbers; also let β, γ, &c. δ represent respectively roots of the equations

$$x^{p^\mu} = 1,\ x^{q^\nu} = 1, \ldots\ x^{r^\lambda} = 1 \ldots\ldots\ldots\ldots (1),$$

then if we assume

$$\alpha = \beta\gamma \ldots \delta \ldots\ldots\ldots\ldots\ldots\ldots (2),$$

it will have m values, because its factors β, γ, &c. δ have respectively p^μ, q^ν, &c. r^λ values; and these values will be the roots of the proposed. It is plain that this expression for α satisfies the proposed; for we have

$$\beta^{p^\mu} = 1,\ \gamma^{q^\nu} = 1,\ \text{\&c.},\ \delta^{r^\lambda} = 1;$$

and consequently

$$\beta^m = 1,\ \gamma^m = 1,\ \text{\&c.},\ \delta^m = 1;\quad \therefore\ \alpha^m = 1.$$

And no two values of α are alike; for, if possible, suppose

$$\beta'\gamma' \ldots \delta' = \beta''\gamma'' \ldots \delta'',$$

and since the quantities $\beta', \gamma', \ldots \delta'$ are not all equal respectively to $\beta'', \gamma'', \ldots \delta''$, let us suppose that β' differs from β''. Now raising this equation to the power $q^\nu \ldots r^\lambda$,

$$(\beta'\gamma' \ldots \delta')^{q^\nu \ldots r^\lambda} = (\beta''\gamma'' \ldots \delta'')^{q^\nu \ldots r^\lambda},$$

and suppressing the factors equal to unity we get

$$\beta'^{q^\nu \ldots r^\lambda} = \beta''^{q^\nu \ldots r^\lambda} \ldots\ldots\ldots\ldots\ldots (3).$$

But β', β'', being two distinct roots of $x^{p^\mu} = 1$, may be expressed respectively by two powers $\beta^{n+n'}$, $\beta^{n'}$ of the same primitive root β of that equation, n and n' being $< p^\mu$.

Substituting these values in (3), we get

$$\beta^{(n+n')q^\nu \ldots r^\lambda} = \beta^{n'q^\nu \ldots r^\lambda} \text{ or } \beta^{nq^\nu \ldots r^\lambda} = 1;$$

from whence it follows that β is a root common to the two equations

$$x^{p^\mu} = 1, \ x^{nq^\nu \dots r^\lambda} = 1,$$

and consequently satisfies the equation $x^t = 1$, t representing the greatest common measure of p^μ and $nq^\nu \dots r^\lambda$. But this common measure t is at most equal to n, and consequently is less than p^μ; therefore β is not as we have supposed, a primitive root of $x^{p^\mu} = 1$; wherefore the assumed formula for α will furnish all the m roots; and if $\beta, \gamma \dots \delta$ be primitive roots of the equations (1) to which they respectively belong, then the value of α given by formula (2) will be a primitive root of the proposed. For if not, then α will satisfy some equation $x^t = 1$ whose degree t is inferior to m; and amongst the prime factors of m there will be at least one that will be contained in t a less number of times than in m; suppose it to be p, then t will be a divisor of

$$p^{\mu-1} q^\nu \dots r^\lambda,$$

and consequently α will be a root of

$$x^{p^{\mu-1} q^\nu \dots r^\lambda} = 1 \dots\dots\dots\dots\dots (4),$$

so that we shall have

$$(\beta\gamma \dots \delta)^{p^{\mu-1} q^\nu \dots r^\lambda} = 1.$$

$$\text{But } \gamma^{q^\nu} = 1, \text{ \&c., } \delta^{r^\lambda} = 1; \ \therefore \ \beta^{p^{\mu-1} q^\nu \dots r^\lambda} = 1;$$

from whence it follows that β is a root of (4), which is impossible since β is a primitive root of the first of the equations (1).

Moreover if any one of the quantities $\beta, \gamma, \dots \delta$ be not a primitive root of the equation to which it belongs, neither will the corresponding value of α be a primitive root of the proposed. For suppose β not to be a primitive root of the first of the equations (1), then we shall have

$$\beta^{p^{\mu-1}} = 1, \ \gamma^{q^\nu} = 1, \text{ \&c., } \delta^{r^\lambda} = 1,$$

$$\therefore \ (\beta\gamma \dots \delta)^{p^{\mu-1} q^\nu \dots r^\lambda} = 1;$$

which shews that $\beta\gamma \dots \delta$ satisfies a binomial equation of a degree inferior to m.

The number of the primitive roots of the proposed may now be computed; for the number of the primitive roots β is

$$p^{\mu}\left(1-\frac{1}{p}\right),$$

that of the primitive roots γ is

$$q^{\nu}\left(1-\frac{1}{q}\right),$$

and so on; therefore the number of the primitive roots of the proposed is

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\dots\left(1-\frac{1}{r}\right).$$

GAUSS'S METHOD OF SOLVING BINOMIAL EQUATIONS.

80. The solution of $x^n - 1 = 0$, by what has been proved, can always be reduced to the case where n is a prime number; and the case of n a prime number, by a method invented by *Gauss*, may be made to depend upon the solution of equations whose degrees do not exceed the greatest prime number which is a divisor of $n-1$. The leading feature of *Gauss's* method is to represent the imaginary roots by a series of powers of any one of them, whose indices form a geometrical instead of an arithmetical progression. Thus, if m be a number (and such, called primitive roots of n, can always be found) whose several powers from 1 to $n-1$, when divided by n, leave different remainders, and α be any imaginary root, then all the roots may manifestly be represented by

$$\alpha^{m},\ \alpha^{m^2},\ \alpha^{m^3},\ \dots\ \alpha^{m^{n-1}};$$

or, since $m^{n-1} = \mu n + 1$, where μ is an integer, by

$$\alpha,\ \alpha^{m},\ \alpha^{m^2},\ \&c.,\ \alpha^{m^{n-2}}.$$

81. The advantage of this mode of representing the roots is, (1) that they can be distributed into periods, each of which,

when continued, will produce the roots of that period in the same order; and (2) that the product of any number of such periods will be equal to the sum of a certain number of periods; the importance of which properties will be seen in the use made of them.

(1) Let $n-1=rs$, r being a prime factor of $n-1$, and let $m^r=h$; then the roots may be written in vertical columns, each consisting of r terms, as follows,

$$\begin{array}{ccccc} \alpha & \alpha^{h} & \alpha^{h^2} & \ldots & \alpha^{h^{s-1}} \\ \alpha^{m} & \alpha^{mh} & \alpha^{mh^2} & \ldots & \alpha^{mh^{s-1}} \\ \alpha^{m^2} & \alpha^{m^2h} & \alpha^{m^2h^2} & \ldots & \alpha^{m^2h^{s-1}} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha^{m^{r-1}} & \alpha^{m^{r-1}h} & \alpha^{m^{r-1}h^2} & \ldots & \alpha^{m^{r-1}h^{s-1}}, \end{array}$$

and if any one of the periods formed by the horizontal rows be continued, the roots in that period will be produced in the same order; thus, if the first row were continued, the indices would be

$h^s=m^{rs}=m^{n-1}=\mu n+1$, $h^{s+1}=m^{rs+r}=(\mu n+1)\,m^r=\mu nh+h$, &c.; and the corresponding roots, α, α^h, &c.

(2) Let any two of the above periods be represented by

$$\alpha^a+\alpha^{ah}+\alpha^{ah^2}+\text{\&c.}+\alpha^{ah^{s-1}}$$
$$\alpha^b+\alpha^{bh}+\alpha^{bh^2}+\text{\&c.}+\alpha^{bh^{s-1}},$$

and let us multiply them together, using each term of the lower line in succession as a multiplier, and starting at that term of the upper line which stands over it, and producing the upper line so as to supply the terms neglected at the beginning, the result is

$$\begin{array}{lllll} \alpha^{a+b} & +\alpha^{ah+b} & +\alpha^{ah^2+b} & +\text{\&c.} & +\alpha^{ah^{s-1}+b} \\ \alpha^{(a+b)h} & +\alpha^{(ah+b)h} & +\alpha^{(ah^2+b)h} & +\text{\&c.} & +\alpha^{(ah^{s-1}+b)h} \\ \alpha^{(a+b)h^2} & +\alpha^{(ah+b)h^2} & +\alpha^{(ah^2+b)h^2} & +\text{\&c.} & +\alpha^{(ah^{s-1}+b)h^2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha^{(a+b)h^{s-1}} & +\alpha^{(ah+b)h^{s-1}} & +\alpha^{(ah^2+b)h^{s-1}} & +\text{\&c.} & +\alpha^{(ah^{s-1}+b)h^{s-1}} \end{array}$$

and therefore, collecting the vertical columns into periods, we get

$$\Sigma(\alpha^a)\,\Sigma(\alpha^b) = \Sigma(\alpha^{a+b}) + \Sigma(\alpha^{ah+b}) + \Sigma(\alpha^{ah^2+b}) + \ldots + \Sigma(\alpha^{ah^{s-1}+b}),$$

or the product of two periods is equal to the sum of s periods; and consequently the product of any number of periods will be equal to the aggregate of a certain number of periods.

Ex. 1. $x^7-1=0$; $6=3.2$, $\therefore r=3$, $s=2$; also 3, 3^2, 3^3, 3^4, 3^5, when divided by 7, leave different remainders, viz. 3, 2, 6, 4, 5; $\therefore m=3$, and the roots are

$$p_1 = \alpha + \alpha^6$$
$$p_2 = \alpha^3 + \alpha^4$$
$$p_3 = \alpha^2 + \alpha^5$$

and $p_1 + p_2 + p_3 = -1$.

Also
$$p_1p_2 = \alpha^4 + \alpha^2 + \alpha^5 + \alpha^3 = p_2 + p_3$$
$$p_2p_3 = \alpha^5 + \alpha^6 + \alpha + \alpha^2 = p_1 + p_3$$
$$p_1p_3 = \alpha^3 + \alpha + \alpha^6 + \alpha^4 = p_1 + p_2;$$
$$\therefore p_1p_2 + p_2p_3 + p_1p_3 = -2$$

and $p_1p_2p_3 = p_1^2 + p_1 + p_2 = 2 + p_3 + p_1 + p_2 = 1$.

Therefore the cubic which has p_1, p_2, p_3, for its roots, is

$$p^3 + p^2 - 2p - 1 = 0.$$

Ex. 2. $x^{17}-1=0$; $16=2.8$, also the powers of 3 from 0 to 15, when divided by 17, leave remainders

1 3 9 10 13 5 15 11 16 14 8 7 4 12 2 6,

$$\therefore p = \alpha + \alpha^9 + \alpha^{13} + \alpha^{15} + \alpha^{16} + \alpha^8 + \alpha^4 + \alpha^2$$
$$q = \alpha^3 + \alpha^{10} + \alpha^5 + \alpha^{11} + \alpha^{14} + \alpha^7 + \alpha^{12} + \alpha^6;$$

then $p + q = -1$, and

$$pq = \alpha^4 + \alpha^{12} + \alpha^{16} + \alpha + \alpha^2 + \alpha^{11} + \alpha^7 + \alpha^5$$
$$\alpha^2 + \alpha^6 + \alpha^8 + \alpha^9 + \alpha + \alpha^{14} + \alpha^{12} + \alpha^{11}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\alpha^8 + \alpha^7 + \alpha^{15} + \alpha^2 + \alpha^4 + \alpha^5 + \alpha^{14} + \alpha^{10}$$

$$= p + q + p + p + p + q + q + q = -4;$$

therefore p and q are roots of $z^2 + z - 4 = 0$.

Next, the periods p, q, may be resolved, respectively into the periods

$$\left.\begin{array}{l} r=\alpha+\alpha^{13}+\alpha^{16}+\alpha^{4} \\ s=\alpha^{9}+\alpha^{15}+\alpha^{8}+\alpha^{2} \end{array}\right\}, \quad \left.\begin{array}{l} t=\alpha^{3}+\alpha^{5}+\alpha^{14}+\alpha^{12} \\ u=\alpha^{10}+\alpha^{11}+\alpha^{7}+\alpha^{6} \end{array}\right\};$$

$$\therefore\ r+s=p,$$

$$\text{and } rs=\left.\begin{array}{l} \alpha^{10}+\alpha^{5}+\alpha^{8}+\alpha^{13} \\ \alpha^{11}+\alpha^{14}+\alpha^{2}+\alpha^{16} \\ \cdots\cdots\cdots\cdots\cdots \\ \alpha^{6}+\alpha^{3}+\alpha^{15}+\alpha \end{array}\right\}=p+q=-1;$$

therefore r, s, are roots of $z^2-pz-1=0$; and similarly t, u, are roots of $z^2-qz-1=0$.

Lastly the periods r, s, t, u, may be resolved, respectively, into

$$\left.\begin{array}{l} r_1=\alpha+\alpha^{16} \\ r_2=\alpha^{13}+\alpha^{4} \end{array}\right\}, \quad \left.\begin{array}{l} s_1=\alpha^{9}+\alpha^{8} \\ s_2=\alpha^{15}+\alpha^{2} \end{array}\right\}, \quad \left.\begin{array}{l} t_1=\alpha^{3}+\alpha^{14} \\ t_2=\alpha^{5}+\alpha^{12} \end{array}\right\}, \quad \left.\begin{array}{l} u_1=\alpha^{10}+\alpha^{7} \\ u_2=\alpha^{11}+\alpha^{6} \end{array}\right\};$$

then $r_1+r_2=r$,

$$r_1r_2=\alpha^{14}+\alpha^{12}+\alpha^{3}+\alpha^{5}=t,$$

$\therefore\ r_1$, r_2, are roots of $z^2-rz+t=0$;

and r_1, the greatest root of this equation, $=\alpha+\dfrac{1}{\alpha}=2\cos\dfrac{\pi}{17}$.

82. Any radical has always as many values as there are units in its index, and these values are obtained by multiplying the arithmetical value of the root of the quantity under the sign, by each of the roots of $+1$ or -1.

For, every root of the equation $x^n \pm a=0$, is an algebraical value of $\sqrt[n]{\mp a}$; but, whatever be $\pm a$, this equation admits n roots all different from one another; therefore the radical $\sqrt[n]{\pm a}$, considered algebraically, will have n different values. When a is real and positive, the equation $x^n=a$ has always one real root α, and the n values of $\sqrt[n]{a}$ will be obtained by multiplying α by each of the n values of $\sqrt[n]{1}$; in like manner, the values of $\sqrt[n]{-a}$ will result from multiplying α by the values of $\sqrt[n]{-1}$.

Hence $\sqrt[m]{a} \times \sqrt[n]{b}$ will have r values, where r is the least common multiple of m and n.

For, let α, β, be the arithmetical values of the radicals,

$$\text{then } \sqrt[m]{a} \times \sqrt[n]{b} = \alpha\beta\,(1)^{\frac{m+n}{mn}};$$

but if $\frac{m+n}{mn}$ be reduced to its lowest terms, the numerator will be an integer and the denominator will be r, the least common multiple of m and n;

$$\therefore\ \sqrt[m]{a} \times \sqrt[n]{b} = \alpha\beta\,(1)^{\frac{1}{r}},$$

which has r different values. Also we see that the extraction of a root of the degree pq, where p and q are prime to one another, is reduced to the extraction of two roots one of the degree p, the other of the degree q. Thus $\sqrt[6]{a} = \sqrt{a}\,.\sqrt[3]{\frac{1}{a}}$; and, α and β being integers positive or negative, so taken that $p\beta + q\alpha = 1$,

$$a^{\frac{1}{pq}} = a^{\frac{p\beta+q\alpha}{pq}} = a^{\frac{\beta}{q}}\,.\,a^{\frac{\alpha}{p}} = \sqrt[q]{a^{\beta}}\,.\,\sqrt[p]{a^{\alpha}}.$$

SECTION V.

ON THE GENERAL SOLUTION OF EQUATIONS OF A DEGREE INFERIOR TO THE FIFTH.

---

83. We shall now direct our attention to those cases of finding the expressions for all the roots of an equation of an assigned degree in terms of its coefficients, the coefficients being general symbols, in which a solution has been effected. These methods, which, as was before observed, succeed only for equations of a degree not exceeding the fourth, are the results of particular artifices; but they are all reducible to one principle, as will be hereafter shewn.

The general expression for the roots of

$$x^n + p_1 x^{n-1} + \&c. = 0,$$

if it could be obtained, would consist, first, of a part affected with radicals, by means of the different values of which, it would be capable of representing all the roots; and, secondly, since the sum of the roots is rational, of a rational part, h, which would be the same for every root; hence, in taking the sum of the roots, the radical parts must destroy one another, and we should have

$$nh = -p_1, \text{ or } h = -\frac{1}{n} p_1,$$

which is the value of the rational part of every root. The general solution of an equation wanting its second term will, consequently, be simpler than that of the corresponding complete equation, as it will have no part unaffected with radicals. Hence in the following instances we shall suppose the equation to be deprived of its second term.

SOLUTION OF A QUADRATIC EQUATION.

84. Let the equation be reduced to the form

$$x^2 + px + q = 0;$$

then this may be transformed into $y^2 = a$, by taking away its second term. For, putting $x = y - \frac{1}{2}p$ (Art. 29), we have

$$y^2 - py + \frac{p^2}{4} + py - \frac{p^2}{2} + q = 0, \text{ or } y^2 = \frac{p^2}{4} - q;$$

$$\therefore\ x = -\frac{p}{2} + y = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

Hence, if $\frac{p^2}{4} > q$, the roots are real; if $\frac{p^2}{4} = q$ they are equal, and $x^2 + px + q = (x + \frac{1}{2}p)^2$ is a perfect square; if $\frac{p^2}{4} < q$, the roots are impossible. Also if α, β, be the two roots,

$$\alpha + \beta = -p, \quad \alpha\beta = q,$$

$$\therefore\ (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = p^2 - 4q.$$

Hence also, any trinomial

$$ax^2 + bx + c \text{ or } a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right)$$

will be resolvable into two real simple factors or not, according as $\frac{b^2}{4a^2} >$ or $< \frac{c}{a}$; and it will be a perfect square when $\frac{b^2}{4a^2} = \frac{c}{a}$, or $b^2 = 4ac$; i.e. when the square of the coefficient of the middle term is equal to four times the product of the coefficients of the extreme terms.

85. Any impossible expression of the form $\alpha \pm \beta\sqrt{-1}$ may be transformed into $r(\cos\theta \pm \sqrt{-1}\sin\theta)$.

For, α and β being real quantities, there always exists an angle θ, such that $\tan\theta = \frac{\beta}{\alpha}$;

$$\text{then } \cos\theta = \frac{\alpha}{\sqrt{\alpha^2+\beta^2}}, \quad \sin\theta = \frac{\beta}{\sqrt{\alpha^2+\beta^2}};$$

if therefore $\sqrt{\alpha^2+\beta^2} = r$, we have

$$\alpha \pm \beta\sqrt{-1} = r(\cos\theta \pm \sqrt{-1}\sin\theta).$$

Hence any pair of imaginary roots of an equation may be represented by the formula $r(\cos\theta \pm \sqrt{-1}\sin\theta)$; and the quantity r, which $= \sqrt{\alpha^2+\beta^2} =$ square root of the product of the roots, and is always real, is called the Modulus of the expression $\alpha + \beta\sqrt{-1}$; and is that quantity by which the impossible roots are estimated, when, as is sometimes requisite, they are compared in regard to magnitude with the real roots.

In the case of the expression,

$$-\frac{p}{2} \pm \sqrt{-1}\sqrt{q - \frac{p^2}{4}},$$

which represents the roots of $x^2 + px + q = 0$ (Art. 84),

$$r = \sqrt{q}, \quad \cos\theta = -\frac{p}{2\sqrt{q}};$$

$$\text{hence, } x^2 + px + q = x^2 - 2r\cos\theta x + r^2;$$

that is, any irreducible quadratic factor of an equation,

$$x^2 + px + q, \text{ where } \frac{p^2}{4} < q,$$

may be transformed into $x^2 - 2r\cos\theta x + r^2$, by making

$$r = \sqrt{q} \text{ and } \cos\theta = -\frac{p}{2\sqrt{q}}.$$

86. To solve an equation of the form

$$x^{2n} + px^n + q = 0.$$

Putting $x^n = y$, we find $y^2 + py + q = 0$.

If this have two real roots a and b, then the $2n$ values of x are the roots of the equations

$$x^n - a = 0, \quad x^n - b = 0.$$

If the roots of the quadratic are imaginary, i. e. if $\frac{p^2}{4} < q$, then, making $r = \sqrt{q}$, and $\cos\theta = \frac{-p}{2\sqrt{q}}$, the proposed equation becomes

$$x^{2n} - 2r\cos\theta x^n + r^2 = 0;$$

$$\text{or } x^{2n} - 2\cos\theta x^n + 1 = 0,$$

changing x^n into $x^n r$, which has already been solved, (p. 26).

SOLUTION OF A CUBIC EQUATION BY CARDAN'S RULE.

87. Let the equation, by Art. 29, be reduced to the form

$$x^3 + qx + r = 0;$$

and put $x = y + z$, that is, suppose x equal to the sum of two other unknown quantities;

$$\therefore\ x^3 = 3yz(y+z) + y^3 + z^3,$$

and therefore the proposed equation becomes

$$(3yz + q)(y+z) + y^3 + z^3 + r = 0.$$

Now since we have two unknown quantities, and have made only one supposition respecting them, namely, that $y + z = x$, we are at liberty to make another; let therefore

$$3yz + q = 0,$$

$$\text{or } y^3z^3 = -\left(\frac{q}{3}\right)^3,\ \therefore\ y^3 + z^3 = -r.$$

Hence y^3, z^3, are the roots of the equation

$$t^2 + rt - \left(\frac{q}{3}\right)^3 = 0,$$

since the coefficient of the second term with its sign changed is equal to their sum, and the last term is equal to their product. Solving this equation, we get

$$t = -\frac{r}{2} \pm \sqrt{\frac{r^2}{4} + \frac{q^3}{27}};$$

$$\therefore\ y^3 = -\frac{r}{2} + \sqrt{\frac{r^2}{4} + \frac{q^3}{27}},\quad z^3 = -\frac{r}{2} - \sqrt{\frac{r^2}{4} + \frac{q^3}{27}};$$

but $x = y + z$,

$$\therefore\ x = \left(-\frac{r}{2} + \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}\right)^{\frac{1}{3}} + \left(-\frac{r}{2} - \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}\right)^{\frac{1}{3}},$$

an expression which (since the cube root of any quantity has three values) contains implicitly the three roots; and the quantities q and r are either real or imaginary.

88. This method only serves for the numerical solution of cubic equations in those cases in which the equation has two impossible roots.

Let the coefficients q and r be real quantities, and let m and n be the arithmetical values of the two surds in the value of x, and 1, α, α^2, the three cube roots of unity; then the three values of y are (Art. 82) m, αm, $\alpha^2 m$, and those of z are n, αn, $\alpha^2 n$. By combining these values two and two to form $y + z$, we shall have nine values of x; the number being tripled by reason of our having employed $y^3 z^3 = -\left(\frac{q}{3}\right)^3$, instead of $yz = -\frac{q}{3}$, the relation arising immediately in the process; and we observe that every combination will satisfy $y^3 z^3 = -\left(\frac{q}{3}\right)^3$, but only three the given condition $yz = -\frac{q}{3}$, which latter are the roots, viz.

$$m + n,\quad \alpha m + \alpha^2 n,\quad \alpha^2 m + \alpha n;$$

or substituting for α, α^2, their values, $-\frac{1}{2}(1 \pm \sqrt{-3})$ (p. 17), the three roots are

$$m + n, \text{ and } -\tfrac{1}{2}\{m + n \pm (m - n)\sqrt{-3}\}.$$

Hence, as long as the expression $\sqrt{\frac{r^2}{4} + \frac{q^3}{27}}$ is possible, the values of m and n are possible, and the equation has one

possible root, the numerical value of which, as also those of the two imaginary roots, may be obtained after somewhat laborious calculations from the above formulæ.

But when the expression $\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}$ is impossible, m and n are impossible, and all the three roots appear under imaginary forms; whereas, the equation, being of an odd degree, has at least one real root; and indeed, since $\frac{r^2}{4}+\frac{q^3}{27}$ is negative, it has (Art. 54) all its roots real; in this case therefore the above formulæ, although algebraical expressions for the roots, cannot on account of the imaginary quantities which they involve, be applied to furnish the numerical values of the roots.

Obs. It is easily seen that the six superfluous values of x above mentioned would be the roots of the proposed equation, supposing q to be successively replaced by αq and $\alpha^2 q$; since each of the relations $yz=-\frac{1}{3}\alpha q$, $yz=-\frac{1}{3}\alpha^2 q$, leads to

$y^3z^3=-\frac{1}{27}q^3$.

Ex. 1. $x^3-3x-110=0$.

$$\frac{q}{3}=-1,\ \frac{r}{2}=-55,$$

$$\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}=\sqrt{(55)^2-1}=12\sqrt{21}=54{\cdot}991;$$

$$\therefore\ x=(55+54{\cdot}991)^{\frac{1}{3}}+(55-54{\cdot}991)^{\frac{1}{3}}$$

$$=4{\cdot}79\ldots+0{\cdot}208\ldots=4{\cdot}999\ldots=5.$$

$$\text{or } x=-\frac{1}{2}\{5\pm(4{\cdot}582\ldots)\sqrt{-3}\}=-\frac{1}{2}(5\pm\sqrt{-62{\cdot}99\ldots})$$

$$=-\frac{1}{2}(5\pm3\sqrt{-7}).$$

Ex. 2. $x^3-12x-65=0$.

$$x=5, \text{ or } -\frac{1}{2}(5\pm 3\sqrt{-3}).$$

Ex. 3. $x^3-2x-5=0$.

$$x=2\cdot0945\ldots, \text{ or } =-1\cdot0172\ldots\pm(1\cdot1362\ldots)\sqrt{-1}.$$

89. In the case of the roots being all real, which, for the reason just stated is called the Irreducible Case, that is, when q is negative, and $\frac{q^3}{27}>\frac{r^2}{4}$, it may be observed that the assumptions in the process

$$y^3+z^3=-r,\ y^3z^3=+\left(\frac{q}{3}\right)^3,$$

are inconsistent with one another; for the product of two real quantities can never exceed the square of half their sum. In this case we can shew that, in the expressions for the roots, the impossible quantities destroy one another, and the three roots are real. For let the values of m^3 and n^3 be represented by $a\pm b\sqrt{-1}$; then, expanding by the binomial theorem, and taking P and Q to denote real functions of a and b, we have

$$(a\pm b\sqrt{-1})^{\frac{1}{3}}=P\pm Q\sqrt{-1};$$

$$\therefore\ m+n=2P,\ m-n=2Q\sqrt{-1};$$

and the three values of x are $2P$, and $-\frac{1}{2}(2P\pm 2Q\sqrt{3})$, which are all real. This mode of proceeding, however, is useless in finding the numerical values of the roots; for if we convert $(a+b\sqrt{-1})^{\frac{1}{3}}$ into a series, P and Q will be expressed by series which rarely converge, and from which we can never obtain the exact values of P and Q; and if we attempt to express the cube root of $a\pm b\sqrt{-1}$ by an expression of the same form, we shall have to solve a cubic of the same kind as the one in question.

Hence *Cardan's* rule succeeds for the following forms, where q and r are essentially positive,

$$x^3 + qx \pm r = 0 \text{ in all cases,}$$

$$x^3 - qx \pm r = 0 \text{ when } \frac{q^3}{27} < \frac{r^2}{4};$$

and it fails for $\quad x^3 - qx \pm r = 0$ when $\dfrac{q^3}{27} > \dfrac{r^2}{4}$,

all the roots of which are real.

90. We may take notice that in *Cardan's* solution two roots can be expressed rationally in terms of the third root and known quantities. For, putting

$$27r^2 + 4q^3 = -\rho^2 \ldots\ldots\ldots\ldots\ldots (1),$$

we get

$$(m-n)\sqrt{-3} = \frac{(m^3-n^3)\sqrt{-3}}{(m+n)^2 - mn} = \frac{\rho}{3(m+n)^2 + q};$$

so that making $m + n = x_1$, and obtaining for ρ its two values from (1), the expression for the other two roots in terms of x_1, is

$$-\frac{1}{2}\left(x_1 + \frac{\rho}{3x_1^2 + q}\right), \text{ or } \frac{-2qx_1^2 + (\rho - 3r)x_1}{2(2qx_1 + 3r)},$$

$$\text{since } x_1^3 + qx_1 + r = 0.$$

Also if we determine Q and R from the identity

$$x^3 + qx + r = Q(2qx + 3r) + R,$$

and then make $x = x_1$, the expression becomes

$$\frac{1}{2}\{-2qx_1^2 + (\rho - 3r)x_1\} \times \frac{-Q}{R} = \frac{1}{2\rho}\{6qx_1^2 - (9r + \rho)x_1 + 4q^2\}.$$

Or, again, determining Q' and R' from the identity

$$x^3 + qx + r = Q'\{6qx^2 - (9r + \rho)x + 4q^2\} + R',$$

and then making $x = x_1$, the expression is transformed into

$$-\frac{1}{2\rho}\frac{R'}{Q'} = -\frac{(9p - \rho)x_1 - 2q^2}{6qx_1 + 9r + \rho}.$$

91. There is one case in which *Cardan's* rule succeeds for the equation $x^3 - qx + r = 0$ when all the roots are real;

it is when two of them are equal, in which case also the roots of the reducing quadratic are equal; for then $m=n$, and the values of x are

$$m+n,\ -\tfrac{1}{2}(m+n),\ -\tfrac{1}{2}(m+n).$$

In this case,

$$\frac{r^2}{4}=\frac{q^3}{27},\ \text{or}\ \frac{r}{2}=\left(\frac{q}{3}\right)^{\frac{3}{2}},$$

$$\therefore\ m^3=n^3=-\frac{r}{2}=-\left(\frac{q}{3}\right)^{\frac{3}{2}};$$

$$\therefore\ m+n=-2\sqrt{\frac{q}{3}},$$

and the roots are

$$-2\sqrt{\frac{q}{3}},\ \sqrt{\frac{q}{3}},\ \sqrt{\frac{q}{3}}.$$

TRIGONOMETRICAL EXPRESSIONS FOR THE ROOTS OF A CUBIC.

By the employment of Trigonometrical formulæ, we obtain simple expressions for the roots of a Cubic, not only in the irreducible case when the algebraical formulæ cease to be of use for computing the numerical values of those roots, but in all the other cases.

92. If in the expression

$$\left(-\frac{r}{2}\pm\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}\right)^{\frac{1}{3}}=\sqrt{\frac{q}{3}}\left\{-\frac{r}{2}\left(\frac{3}{q}\right)^{\frac{3}{2}}\pm\sqrt{\frac{r^2}{4}\left(\frac{3}{q}\right)^{3}+1}\right\}^{\frac{1}{3}},$$

we put $\cot\phi=\dfrac{r}{2}\left(\dfrac{3}{q}\right)^{\frac{3}{2}}$, it becomes $\sqrt{\dfrac{q}{3}}(-\cot\phi\pm\operatorname{cosec}\phi)^{\frac{1}{3}}$.

Hence, reducing, the real root of $x^3+qx+r=0$ is

$$\sqrt{\frac{q}{3}}\left(\tan^{\frac{1}{3}}\frac{\phi}{2}-\cot^{\frac{1}{3}}\frac{\phi}{2}\right);$$

which, by putting $\tan\dfrac{\phi}{2}=\tan^3\theta$, may be further transformed into

$$-2\sqrt{\frac{q}{3}}\cot 2\theta.$$

Similarly, the real root of $x^3 - qx + r = 0$, $\frac{q^3}{27} < \frac{r^2}{4}$, becomes (by putting $\operatorname{cosec}\phi = \frac{r}{2}\left(\frac{3}{q}\right)^{\frac{3}{2}}$, $\tan\frac{\phi}{2} = \tan^3\theta$),

$$-2\sqrt{\frac{q}{3}}\operatorname{cosec} 2\theta.$$

Also, in the irreducible case, $x^3 - qx \pm r = 0$, $\frac{q^3}{27} > \frac{r^2}{4}$, the expression

$$\mp\frac{r}{2} \pm \sqrt{\frac{r^2}{4} - \frac{q^3}{27}} = \left(\frac{q}{3}\right)^{\frac{3}{2}}\left\{\mp\frac{r}{2}\left(\frac{3}{q}\right)^{\frac{3}{2}} \pm \sqrt{-1}\left(1 - \frac{27r^2}{4q^3}\right)^{\frac{1}{2}}\right\},$$

by making $\cos\phi = \pm\frac{r}{2}\left(\frac{3}{q}\right)^{\frac{3}{2}}$, becomes equally

$$\left(\frac{q}{3}\right)^{\frac{3}{2}}(-\cos\phi \pm \sqrt{-1}\sin\phi),$$

$$\text{or } \left(\frac{q}{3}\right)^{\frac{3}{2}}\{\cos(\pi \pm \phi) \pm \sqrt{-1}\sin(\pi \pm \phi)\};$$

and therefore the three values of x are

$$-2\sqrt{\frac{q}{3}}\cos\frac{\phi}{3},\quad 2\sqrt{\frac{q}{3}}\cos\left(\frac{\pi \pm \phi}{3}\right).$$

SOLUTION OF A BIQUADRATIC EQUATION BY DES CARTES'S METHOD.

93. Let the proposed equation be reduced to the form

$$x^4 + qx^2 + rx + s = 0;$$

and as the first member may be always regarded as the product of two real quadratic factors, we may assume it

$$= (x^2 + px + f)(x^2 - px + g)$$
$$= x^4 + (g + f - p^2)x^2 + (pg - pf)x + fg$$

(effecting the multiplication), where the coefficients of the second terms, p and $-p$, are equal and of opposite signs, because the second term of the proposed equation is wanting, that is, the sum of its roots is zero. Hence, equating coefficients,

$$g+f-p^2=q,\ pg-pf=r,\ fg=s,$$

$$\text{or } g+f=q+p^2,\ g-f=\frac{r}{p};$$

$$\therefore\ 2g=q+p^2+\frac{r}{p},\ 2f=q+p^2-\frac{r}{p};$$

$$\therefore\ 4fg=q^2+2qp^2+p^4-\frac{r^2}{p^2}=4s,$$

$$\text{or } p^6+2qp^4+(q^2-4s)\,p^2-r^2=0,$$

the equation for determining p, which rises to the sixth degree, because a polynomial of four dimensions, may have (Art. 17) $\frac{4\,.\,3}{1\,.\,2}$, or six divisors of the second order. Also, because the values of p are the sums of every two roots of the proposed biquadratic, and because the sum of these roots is zero, and therefore the sum of any two is equal and of a contrary sign to the sum of the other two, therefore the values of p will be in pairs differing only in sign; this is the reason why the equation for determining p involves only even powers of p, and may therefore be depressed to a cubic by putting $p^2=y$. The reducing cubic is

$$y^3+2qy^2+(q^2-4s)\,y-r^2=0,$$

which (Art. 10) has necessarily one real positive root; let this be e^2, then the four values of x are contained in the quadratic equations

$$x^2+ex+\frac{1}{2}\left(q+e^2-\frac{r}{e}\right)=0,$$

$$x^2-ex+\frac{1}{2}\left(q+e^2+\frac{r}{e}\right)=0.$$

Ex. $$x^4 - 3x^2 - 42x - 40 = 0.$$

Here $q = -3,\ r = -42,\ s = -40$;

and the reducing cubic is

$$y^3 - 6y^2 + 169y - (42)^2 = 0,$$

which has a root $= 9$ (Art. 67),

$$\therefore\ e = 3;\ \therefore\ x^2 + 3x + 10 = 0,\ x^2 - 3x - 4 = 0;$$

the roots of these quadratics $-\frac{1}{2}\left(3 \pm \sqrt{-31}\right)$, -1, 4, are the roots of the proposed equation.

94. The reducing cubic will have all its roots real, unless two of the roots of the proposed biquadratic are possible and unequal, and two impossible.

For the square of the sum of any two roots of the proposed is a root of the reducing cubic; if therefore the proposed have all its roots real, the reducing cubic will have all its roots real; or if the proposed have all its roots imaginary, and therefore of the form

$$\alpha + \beta\sqrt{-1},\ \alpha - \beta\sqrt{-1},\ -\alpha + \beta'\sqrt{-1},\ -\alpha - \beta'\sqrt{-1},$$

since their sum is zero, then the square of the sum of every two will be real, and therefore the cubic will have all its roots real. But if the proposed have two real unequal roots, and two imaginary roots, and therefore of the forms

$$\alpha + \beta\sqrt{-1},\ \alpha - \beta\sqrt{-1},\ -\alpha + \gamma,\ -\alpha - \gamma,$$

then the square of the sum of a real and an imaginary root will be imaginary, and therefore the cubic will have one and consequently two imaginary roots. As it is only in the latter case that a numerical solution of the reducing cubic can be obtained, therefore *Des Cartes's* method can only be applied to those cases in which two roots of the biquadratic are possible and unequal, and two impossible.

It will be observed that in the latter case, if the two real roots are equal to one another, i.e. if $\gamma = 0$, the cubic will have all its roots real; but as two of them are equal, it can still be solved.

95. If the roots of the reducing cubic can be obtained, and are put under the forms $(2\alpha)^2$, $(2\beta)^2$, $(2\gamma)^2$, then the four roots of the biquadratic are

$$-(\alpha+\beta+\gamma),\ \beta+\gamma-\alpha,\ \alpha+\gamma-\beta,\ \alpha+\beta-\gamma.$$

For, $-\frac{1}{2}q=\alpha^2+\beta^2+\gamma^2$, and $r^2=(8\alpha\beta\gamma)^2$;

$$\text{let } p^2=(2\alpha)^2, \text{ or } p=\pm 2\alpha;$$

therefore, taking the upper sign,

$$f=\frac{1}{2}\left(q+p^2-\frac{r}{p}\right)=-(\alpha^2+\beta^2+\gamma^2)+2\alpha^2-2\beta\gamma$$

$$=\alpha^2-(\beta+\gamma)^2;$$

therefore the first reducing quadratic is

$$x^2+2\alpha x+\alpha^2-(\beta+\gamma)^2=0,$$

which gives for x the values

$$-(\alpha+\beta+\gamma),\ \beta+\gamma-\alpha;$$

similarly, the other quadratic, taking $p=-2\alpha$, is

$$x^2-2\alpha x+\alpha^2-(\beta-\gamma)^2=0,$$

which gives the other values

$$\alpha+\gamma-\beta,\ \alpha+\beta-\gamma.$$

Hence the roots of the biquadratic are symmetrical functions of the roots of the reducing cubic; and whatever root of the reducing cubic is used in the process, the same values of x are obtained.

SOLUTION OF A COMPLETE BIQUADRATIC BY FERRARI'S METHOD.

96. Let the equation be

$$x^4+px^3+qx^2+rx+s=0,$$

and let it be supposed the same as

$$\left(x^2+\frac{p}{2}x+m\right)^2-(kx+l)^2=0,$$

where k, l, m are unknown, and are to be determined so as to make the latter equation coincide with the proposed. Now

$$\left(x^2+\frac{p}{2}x+m\right)^2=x^4+px^3+\left(\frac{p^2}{4}+2m\right)x^2+pmx+m^2$$
$$-(kx+l)^2= \qquad -k^2x^2-2klx-l^2;$$

therefore, by comparing this with the proposed, we have, to determine k, l, m, the equations

$$\frac{p^2}{4}+2m-k^2=q, \quad pm-2kl=r, \quad m^2-l^2=s.$$

Substituting, in the second, the values of k and l obtained from the first and third, we get for the reducing cubic

$$8m^3-4qm^2+(2pr-8s)\,m-p^2s+4qs-r^2=0\ldots(1),$$

which will necessarily give one real value for m; then k and l are known; and we find the two reducing quadratics

$$x^2+\left(\frac{p}{2}+k\right)x+m+l=0,$$

$$x^2+\left(\frac{p}{2}-k\right)x+m-l=0.$$

Ex. $x^4+x^3-4x^2-4x+1=0$.

The reducing cubic is

$$8m^3+16m^2-16m-33=0,$$

in which a value of $2m$ is -3; therefore $k=\frac{1}{2}\sqrt{5}$, $l=\frac{1}{2}\sqrt{5}$; and the proposed equation is decomposed into

$$x^2+\tfrac{1}{2}(1+\sqrt{5})\,x+\tfrac{1}{2}(-3+\sqrt{5})=0,$$
$$x^2+\tfrac{1}{2}(1-\sqrt{5})\,x+\tfrac{1}{2}(-3-\sqrt{5})=0.$$

97. In this method the reducing cubic will have all its roots real, unless two roots of the biquadratic are possible and two impossible; for suppose the roots to be α, β, γ, δ; and suppose any two α, β, to satisfy the first reducing quadratic, and consequently γ, δ, the second,

$$\therefore\ m+l=\alpha\beta,\ m-l=\gamma\delta;$$

$\therefore\ m = \frac{1}{2}(\alpha\beta + \gamma\delta)$, and the other values of m must be

$$\tfrac{1}{2}(\alpha\gamma + \beta\delta),\ \tfrac{1}{2}(\alpha\delta + \beta\gamma).$$

Hence if α, β, γ, δ, be either all possible, or all impossible, the values of m are real; but if two roots of the biquadratic be possible and two impossible, then two values of m will be impossible, and the reducing cubic may be solved by *Cardan's* rule. In the latter case, however, if the two real roots are equal, the cubic will have all its roots real; but it may be solved, because two of them will be equal.

If in (1) we substituted for $2m$ the value $k^2 - \frac{1}{4}p^2 + q$, it would be transformed into an equation of the sixth degree in k, but containing only even powers of k, and might be taken for the reducing equation; then since

$$\alpha + \beta = -\tfrac{1}{2}p - k,\ \gamma + \delta = -\tfrac{1}{2}p + k,$$

therefore $-2k = \alpha + \beta - \gamma - \delta$, the expression for the roots of the reducing equation in k; which is a linear function of the roots of the proposed, and can, by permuting those roots, assume six values, equal two and two and of contrary signs.

SOLUTION OF A BIQUADRATIC BY EULER'S METHOD.

98. Let the equation be reduced to the form

$$x^4 + qx^2 + rx + s = 0,$$

and assume $x = y + z + u$;

$$\therefore\ x^2 = y^2 + z^2 + u^2 + 2(yz + yu + zu),$$

$$\text{or } x^2 - (y^2 + z^2 + u^2) = 2(yz + yu + zu);$$

$$\therefore\ x^4 - 2x^2(y^2 + z^2 + u^2) + (y^2 + z^2 + u^2)^2 = 4(y^2z^2 + y^2u^2 + z^2u^2) + 8yzu(y + z + u),$$

or, replacing $y + z + u$ by x, and transposing,

$$x^4 - 2x^2(y^2 + z^2 + u^2) - 8yzux + (y^2 + z^2 + u^2)^2 - 4(y^2z^2 + y^2u^2 + z^2u^2) = 0.$$

In order that this may coincide with the proposed, we must have

$$q = -2(y^2 + z^2 + u^2), \quad r = -8yzu,$$
$$s = (y^2 + z^2 + u^2)^2 - 4(y^2z^2 + y^2u^2 + z^2u^2);$$

$$\text{or } y^2 + z^2 + u^2 = -\frac{q}{2}, \quad y^2z^2 + y^2u^2 + z^2u^2 = \frac{q^2 - 4s}{16},$$

$$yzu = -\frac{r}{8}, \quad \text{or } y^2z^2u^2 = \frac{r^2}{64};$$

hence y^2, z^2, u^2, are the roots of the cubic

$$t^3 + \frac{q}{2}t^2 + \frac{q^2 - 4s}{16}t - \frac{r^2}{64} = 0.$$

Let t^2, t'^2, t''^2, denote the three values of t in this equation;

$$\therefore\ y = \pm t, \quad z = \pm t', \quad u = \pm t'';$$

which six values, combined three and three, would give 8 values of $y + z + u$ or x, instead of 4; the number being doubled because we have used $y^2z^2u^2 = \frac{r^2}{64}$, instead of the given condition $yzu = -\frac{r}{8}$ which only allows those values of y, z, u, to be combined which give, when multiplied together, a result with a contrary sign to r.

Hence if r be negative, there must be either two negative quantities, or none, in every combination; and if r be positive, there must be either two positive quantities, or none, in every combination representing a root. Therefore, in the former case, that is, when r is negative, the roots are

$$t - t' - t'', \quad t' - t - t'', \quad t'' - t - t', \quad t + t' + t'';$$

and in the latter case, when r is positive, the roots are

$$t + t' - t'', \quad t + t'' - t', \quad t' + t'' - t, \quad -t - t' - t'';$$

and it will be observed, that the second set of roots results from the first, by changing the sign of any one of the quantities t, t', t''.

99. In this case also, the reducing cubic will have all its roots real, except when the proposed has two possible and two impossible roots.

Since the last term of the reducing cubic is essentially negative, it will always have one real positive root t^2, and the remaining roots will be either both positive, both negative, or impossible; that is, of the forms

$$t'^2,\ t''^2;\ -t'^2,\ -t''^2;\ \text{or}\ \rho^2\,(\cos 2\theta \pm \sqrt{-1}\,\sin 2\theta).$$

Hence, according as the reducing cubic has three positive roots, two negative roots, or impossible roots, the biquadratic

$$x^4 + qx^2 - rx + s = 0$$

will have its roots respectively of the forms

$$t \pm (t' + t''),\ \ -t \pm (t' - t'');$$
$$t \pm \sqrt{-1}\,(t' - t''),\ \ -t \pm \sqrt{-1}\,(t' + t'');$$
$$t \pm 2\rho \cos\theta,\ \ -t \pm \sqrt{-1}\,2\rho \sin\theta.$$

In the case of the equation

$$x^4 + qx^2 + rx + s = 0,$$

we must change the sign of t in the above expressions, and the results will be its roots.

If $2\theta = \pi$, or the two real roots of the biquadratic become equal, then, as before, the reducing cubic has three real roots, two of which are alike.

Lagrange's method of solving both cubic and biquadratic equations will be given in Section X. He shews that all the other methods, though different in appearance, ultimately involve the same principle: viz. that of making the solution of the proposed equation depend upon that of a reducing equation whose roots are linear functions of the roots of the proposed equation, and of the roots of unity of the same degree as the proposed equation. For equations of a higher degree than the fourth, the dimension of the reducing equation exceeds that of the proposed.

The solution of the general equation of the fifth degree is, as has been stated, impossible; but in Section VIII. we shall shew that it can be transformed, so as to want any three consecutive terms between the first and the last.

SECTION VI.

ON THE SEPARATION OF THE ROOTS OF EQUATIONS.

100. THE propositions in the preceding sections lead us to several important conclusions relating to the nature and the limits of the roots of every equation; and for equations of low degrees and of certain particular forms, the methods detailed in them (especially that of Art 49) will actually determine the number and situation of all the real roots; that is, two quantities between which each of the real roots lies. They still, however, leave unsolved the main problem, which is to discover the number and situation of the real roots of an equation of any degree. This we shall now endeavour to effect by the methods proposed by *Sturm* and *Fourier*, which are among the greatest improvements recently made in the Theory of Equations.

STURM'S METHOD OF SEPARATING THE ROOTS.

101. By performing a process nearly the same as that of finding the greatest common measure of $f(x)$, and its first derived function $f'(x)$, a series of expressions may be obtained, in which, by simply substituting a and b successively for x, the number of roots of $f(x) = 0$, which lie between a and b, may be exactly determined. The enunciation and proof are as follows.

Let $f(x)=0$ be an equation of n dimensions cleared of equal roots, $f_1(x)$ the first derived function of $f(x)$; and let the process of finding the greatest common measure of $f(x)$ and $f_1(x)$ be performed with the condition that the remainder after each operation has its sign changed, and so modified is used for the divisor of the next operation*; and let $f_2(x)$, $f_3(x)$, ...$f_n(x)$ be the series of modified remainders; then the difference of the number of changes of sign, in the results of the substitutions of a and b for x in the series of quantities

$$f(x),\ f_1(x),\ f_2(x),\ \ldots f_n(x),\quad (1),$$

expresses the number of real roots of $f(x)=0$, which lie between a and b.

Calling the successive quotients q_1, q_2, &c., we shall have the equations

$$f(x)=q_1 f_1(x)-f_2(x)$$
$$f_1(x)=q_2 f_2(x)-f_3(x)$$
$$.\ .\ =\ .\ .\ .\ .\ .$$
$$f_{m-1}(x)=q_m f_m(x)-f_{m+1}(x)$$
$$.\ .\ =\ .\ .\ .\ .\ .\ .$$
$$f_{n-2}(x)=q_{n-1} f_{n-1}(x)-f_n(x),$$

$f_n(x)$ being necessarily a number (Art. 60), since $f(x)=0$ has no equal roots; which shew,

(1) That no value of x can make two consecutive functions $f_{m-1}(x)$ and $f_m(x)$, vanish; for then $f_{m+1}(x)$ and all the succeeding functions would vanish, which is impossible, since the last is a number.

(2) That any value which makes a function, $f_m(x)$, vanish, reduces the two adjacent ones to the same numerical value with different signs.

* This changing of the signs of the remainders, which would be indifferent if the object was only to discover the greatest common measure of $f(x)$ and $f_1(x)$, is essential to the method about to be explained.

Now if in series (1) we make $x = c$, and then suppose c to assume all possible ascending values from $-\infty$ to $+\infty$, the resulting series of signs will have two states of permanence; one, as long as c is nearer to $-\infty$, and the other after c is nearer to $+\infty$, than any quantity which makes any one of the expressions in series (1) vanish; and between these states, whenever any of the expressions vanish, alterations in the order or number of changes of signs, or in both, will occur; and we shall shew that when x passes through a quantity which makes one or more of the auxiliary functions vanish, it is only the order but not the number of changes which is affected; and that when x passes through a root of $f(x) = 0$, then a change of sign is lost.

First, let $x = c$ make only one of the auxiliary functions, $f_m(x)$, vanish, without making $f(x)$ vanish; then to discover the effect, upon the series of signs, of passing through c, we must compare the results of substituting $c - h$ and $c + h$ for x, h being as small as ever we please; therefore we may suppose h so small that neither $f(x)$ nor any of the auxiliary functions can vanish for values between $c - h$ and $c + h$, and that the sign of any series ascending by powers of h depends upon that of its first term. Hence the only part of series (1) in which the passage from $c - h$ to $c + h$ can produce any effect upon the series of signs, is

$$f_{m-1}(x),\ f_m(x),\ f_{m+1}(x),$$

in which, if we write $c - h$ for x, expand the results (Art. 27), and reserve only that term of each on which its sign depends, we have

$$f_{m-1}(c),\ -hf'_m(c),\ f_{m+1}(c),$$

which, since by (2) the extremes have different signs, give a change and continuation, whatever be the sign of the middle term; and these, by changing the sign of h, will be replaced by a continuation and change; i. e. the passage from $c - h$ to $c + h$, through a root of $f_m(x) = 0$, causes an alteration in the

order but not in the number of changes. If the same value of x made an auxiliary function vanish in another part of the series, since by (1) adjacent terms can never vanish, the same considerations would shew that no change of sign could be lost or gained.

Secondly, let $x=c$ be a root of $f(x)=0$; the substitution of $c-h$ for x in $f(x)$ and $f_1(x)$, (taking h so small that the sign of the whole of each series depends upon that of its first term, and writing down only the first terms) gives

$$-hf'(c),\ f_1(c),\ \text{or}\ -hf'(c),\ f'(c),$$

which have different signs; but if the sign of h be changed they have the same signs; therefore the two functions $f(x)$, $f_1(x)$, which for $x=c-h$ give a change, for $x=c+h$ give a continuation; and therefore, in passing through a root of $f(x)=0$, a change of signs is lost. If at the same time that $f(x)$ becomes zero, any number of auxiliary functions vanished, since no two of them could be adjacent, it would follow, as before, that no change of sign could be lost in the parts of the series where they are situated.

Since then a change of signs is lost every time the substituted quantity passes through a root of $f(x)=0$; and since a change cannot be lost in any other way, nor one ever introduced; it follows, that the excess of the number of changes given by $x=a$, above that given by $x=b$, $(a<b)$, is exactly equal to the number of real roots of $f(x)=0$ lying between a and b.

Obs. Before proceeding to apply this method to particular instances, there are several remarks to be made; by attending to which, the nature of the roots in every case becomes known from the mere inspection of the auxiliary functions; and the separation of the real roots is, in many cases, greatly facilitated. If by either of the substitutions of a and b for x, one of the auxiliary functions, $f_m(x)$, is reduced to

zero, it may be neglected in estimating the number of changes; for in that case, as has been shewn, the adjacent functions will have different signs; and therefore the evanescent function, with whatever sign it is taken, will cause the three to furnish but one change, and may therefore be omitted without affecting the number of changes.

102. If we substitute $-\infty$ and $+\infty$ for x, or, which comes to the same thing, if we form the first or leading terms of $f(x)$, $f_1(x) \dots f_n(x)$ into a series, and then change x into $-x$, the difference of the number of changes of sign in the two resulting series will express the total number of real roots.

103. Since, in finding the greatest common measure of $f(x)$ and $f_1(x)$, each remainder is at least one dimension lower than the preceding, the auxiliary functions will usually be n in number, the same as the degree of the equation, and of the several dimensions from $n-1$ to 0. When none of the auxiliary functions are wanting, and the first terms of $f(x)$, $f_1(x)$, $f_2(x)$, $\dots f_n(x)$ have all the same sign, $-\infty$ gives n changes, and $+\infty$ gives no changes, therefore all the roots of $f(x)=0$ are real.

104. On the contrary, when none of the auxiliary functions are wanting and the first terms have not all the same sign, there will be as many pairs of imaginary roots as there are changes in the signs of the first terms.

In the series formed by the first terms of the $n+1$ quantities $f(x)$, $f_1(x)$, $\dots f_n(x)$, let there be s changes and therefore $n-s$ continuations, then these are the same as the numbers of changes and continuations produced by the substitution of $+\infty$ for x; now write $-\infty$ for x in the same series, then every change will be replaced by a continuation, and *vice versâ*; and therefore there will be $n-s$ changes, a number necessarily greater than s, since the number of changes diminishes as the

quantity substituted increases; that is, in passing from $-\infty$ to $+\infty$, $n-2s$ changes are lost; therefore the equation has only $n-2s$ real roots, and therefore $2s$ imaginary roots; or as many pairs of imaginary roots as there are changes of sign in the series formed by the first terms of the $n+1$ quantities

$$f(x),\ f_1(x), \dots f_n(x).$$

105. If one of the auxiliary functions, $f_m(x)$, be such as to preserve the same sign for all values of x between a and b, then in ascertaining the number of roots between a and b, we may neglect all the auxiliary functions after $f_m(x)$. Because (since in general the passage through a quantity which makes one of the auxiliary functions vanish, causes an alteration only in the order but not in the number of changes, and since $f_m(x)$ preserves the same sign for all values of x between a and b) the number of changes presented by the series of auxiliary functions which follow $f_m(x)$ cannot be altered by the substitution of any value of x between those limits; and therefore the difference in the number of changes given by the substitutions of a and b will be the same, whether we take the auxiliary functions that follow $f_m(x)$ into account or not.

Hence if $f_m(x)=0$ have all its roots impossible, since $f_m(x)$ will preserve the same sign for all values of x, we may arrest the process at it, and confine our attention to the $m+1$ functions,

$$f(x),\ f_1(x),\ f_2(x), \dots f_m(x);$$

and, as in the former case, if the first terms of these offer s changes of sign, there will be only $m-2s$ real roots, and the rest will be imaginary.

106. We shall now give some applications of this theorem.

Having formed the auxiliary functions

$$f_1(x),\ f_2(x),\ f_3(x), \dots f_n(x),$$

then if none of them be wanting, and their leading terms be all positive, (for the leading term of $f(x)$ is necessarily so) the equation will have all its roots real; but if the leading terms are not all positive, the equation will have as many pairs of imaginary roots as there are changes of sign in them. But if some of the auxiliary functions are wanting, the number of real roots must be determined by substituting $-\infty$ and $+\infty$ for x in their leading terms, and taking the difference between the numbers of changes resulting from these substitutions. This determines the *number* of real roots. To determine their *situations* we must substitute 0, 1, 2, 3, &c., for x in the series

$$f(x),\ f_1(x),\ f_2(x),\ \ldots f_n(x),$$

till we arrive at a number which gives the same number of changes as is given by $+\infty$; then, by noting the difference in the number of changes produced by the extreme substitutions, we determine the number of + roots; and by noting those consecutive integers between which one or more changes are lost, we determine the integral limits between which the positive roots are situated, either singly or in groups; and in the latter case, we must substitute fractional quantities lying between the integral limits, smaller and smaller, till the complete separation of each group of roots is effected.

In like manner for the negative roots, we must substitute 0, -1, -2, -3, &c., till we arrive at a number which gives the same number of changes as is given by $-\infty$; then the total number of negative roots, and an interval in which each is situated, may be determined, exactly in the same manner as for the positive roots. And in order to diminish the labour of the process, it must be observed that when, in forming the auxiliary functions, we come to one (that of the second degree, for instance, when the conditions of Art. 84 are fulfilled) which is incapable of changing its sign for any real value of x, we may take it for the last of the auxiliary functions.

Ex. 1. $f(x) = x^3 - 7x + 7 = 0.$

$$f_1(x) = 3x^2 - 7 \,)\, 3x^3 - 21x + 21 \,(\, x$$
$$3x^3 - 7x$$
$$\overline{\quad - 14x + 21,}$$

$$\text{or } f_2(x) = 2x - 3 \,)\, 6x^2 - 14 \,(\, 3x + \frac{9}{2}$$
$$6x^2 - 9x$$
$$\overline{9x - 14}$$
$$9x - \frac{27}{2}$$
$$\overline{\quad - \tfrac{1}{2}}$$

or $f_3(x) = +1$. Hence $f(x) = x^3 - 7x + 7$,
$f_1(x) = 3x^2 - 7$, $f_2(x) = 2x - 3$, $f_3(x) = 1$.

Since the leading terms are all positive, and none of the auxiliary functions are wanting, the roots are all possible. Also, since 2 makes all the functions positive, the substitutions for the purpose of separating the roots may begin from thence; therefore, making $x = 2, 1, 0, -1, -2$, &c., the signs are as follows:

	$f(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$
(2)	+	+	+	+
(1)	+	−	−	+
(0)	+	−	−	+
(−1)	+	−	−	+
(−2)	+	+	−	+
(−3)	+	+	−	+
(−4)	−	+	−	+

We may stop here, because the signs are the same as those given by $-\infty$. Since the first line gives no changes,

and the second line two, two roots lie between 2 and 1; also the last line has one more change than the preceding, therefore one root lies between -3 and -4.

To separate the two roots which lie between 1 and 2, let $x=\frac{3}{2}$; then the resulting series of signs is $- - 0 +$, which has one more change than the first line, and one less than the second, (whatever sign we give to the zero); therefore one root lies between 1 and 1·5, and another between 1·5 and 2.

Ex. 2. $f(x)=x^n-nqx+(n-1)r=0$, where q is essentially positive.

$$f_1(x)=nx^{n-1}-nq$$

$$x^{n-1}-q\,)\,x^n-nqx+(n-1)\,r\,(x$$
$$\underline{x^n-qx\qquad\qquad\qquad}$$
$$-(n-1)\,qx+(n-1)\,r$$

or $f_2(x)=x-\frac{r}{q}$, rejecting the positive factor $(n-1)\,q$.

But the remainder, after dividing

$$x^{n-1}-q \text{ by } x-\frac{r}{q}, \text{ is (Art. 6) } \left(\frac{r}{q}\right)^{n-1}-q;$$

$$\text{therefore } f_3(x)=-\left(\frac{r}{q}\right)^{n-1}+q.$$

Now supposing $f_3(x)$ positive, $+\infty$ gives no change, and $-\infty$ gives two changes when n is even, and three changes when n is odd. Hence if $q^n>r^{n-1}$, the proposed equation has two, or three real roots, according as n is even or odd. Similarly, if $q^n<r^{n-1}$, $+\infty$ gives one change, and $-\infty$ one, or two changes, according as n is even or odd; and therefore the equation has no real root, or one real root, according as n is even or odd. These results agree with those found at p. 61.

Ex. 3. $f(x) = 2x^4 - 13x^2 + 10x - 19 = 0,$

$$f_1(x) = 4x^3 - 13x + 5;$$

and we find

$$f_2(x) = 13x^2 - 15x + 38.$$

But the roots of $13x^2 - 15x + 38 = 0$ are imaginary, because $(15)^2 < 4 . 13 . 38$ (Art. 84); therefore it is sufficient to consider the above three functions, and since their leading terms give two changes for $x = -\infty$, and no change for $x = +\infty$, the equation has only two real roots.

Ex. 4. $f(x) = x^4 - 4x^3 - 3x + 23 = 0.$

$$f_1(x) = 4x^3 - 12x^2 - 3, \ f_2(x) = 12x^2 + 9x - 89,$$

$$f_3(x) = -491x + 1371, \ f_4(x) = -7157932.$$

Here there are only two real roots, of which, one lies between 2 and 3, and the other between 3 and 4.

107. It is plain that if we can obtain, by whatever means, auxiliary functions satisfying the conditions of Art. 101, we may separate the roots. Thus if we represent the first member of an equation of the n^{th} degree by V_n, and form equations by the law $V_n = xV_{n-1} - V_{n-2}$ (1), assuming $V_0 = a$, $V_1 = x + b$; so that

$$V_2 = x^2 + bx - a, \ V_3 = x^3 + bx^2 - (a+1)x - b, \text{ \&c.};$$

then $V_{n-1}, V_{n-2}, \dots V_1, V_0$ will evidently serve as auxiliary functions to $V_n = 0$; and every equation formed in this way will have all its roots real provided a be positive. If $a = 2$, $b = 0$, we fall upon the equation of Art. 70,

$$V_n = x^n - nx^{n-2} + \frac{n(n-3)}{1 . 2} x^{n-4} - \text{\&c.} = 0;$$

and from (1) it is easily seen that for

$$x = -2, \ V_0 = 2, \ V_1 = -2, \ V_2 = 2, \text{ \&c.};$$

$$\text{and for } x = 2, \ V_0 = V_1 = V_2 = V_3 = 2;$$

therefore n changes are lost in passing from -2 to $+2$, and consequently the n roots of $V_n = 0$ lie between the same numbers. Similarly, if $a = b = 1$, we fall upon the equation

$$U_n = x^n + x^{n-1} - (n-1)\,x^{n-2} - (n-2)\,x^{n-3} + \&c. = 0\,;$$

and it may be shewn, in the same way, that the n roots of $U_n = 0$ are situated between -2 and 2.

It is manifest that in *Sturm's* method, the labour of forming the auxiliary functions increases very rapidly with the degree of the equation; since however they can always be formed, the method will enable us infallibly to determine, not merely a limit to the number, but the absolute number of real roots in any proposed equation, and the consecutive integers between which they lie either singly or in determined groups; as also the intervals in which no real root can be situated; but when two or more roots are indicated in any interval, if they lie very near to one another, although the method leaves no doubt of the existence of the roots, it may be very difficult to subdivide the interval sufficiently to completely separate them.

FOURIER'S METHOD OF SEPARATING THE ROOTS.

108. We shall now give another method of separating the roots proposed by *Fourier*, which has the recommendation that the auxiliary functions employed in it are $f(x)$ and its successive derived functions, which can be formed by inspection; so that the method can be applied nearly with equal ease to an equation of any degree; in particular, the intervals in which no real root can be situated are, by *Fourier's* method, immediately assigned. The objection to this method is that, by its immediate application, we only find a limit which the number of real roots in a given interval cannot exceed, and not the absolute number; and that the subsidiary propositions by which this defect is supplied, are

not of the same simple character as the original Theorem. The enunciation and proof are as follows.

The number of real roots of $f(x) = 0$ which lie between two numbers a and b, cannot exceed the difference between the number of changes of sign in the results of the substitutions of a and b for x, in the series formed by $f(x)$ and its derived functions: viz.

$$f(x),\ f'(x),\ f''(x),\ \ldots f^{n}(x);$$

and when it falls short of that difference, it will be by an even number.

If none of the equations

$$f(x) = 0,\ f'(x) = 0,\ \&c.$$

have a root between a and b, it is manifest that the substitution of a and b, and of any intermediate quantity, in $f(x)$, $f'(x)$, &c., will always produce exactly the same series of signs; but if any of these equations have roots between a and b, then changes in the series of signs will occur in substituting gradually ascending quantities from a to b; our object is to show that by such substitutions the number of changes of signs can never increase; and that one change will be lost every time the substituted quantity passes through a real root of $f(x) = 0$; this we shall do, by examining, separately, each of the cases in which the series of signs can be affected; namely, (1) when $f(x)$ alone vanishes; (2) when some derived function, $f^{m}(x)$, alone vanishes; (3) and (4) when some group of derived functions, of which $f(x)$ either is not, or is, a part, alone vanishes; and lastly, when several, or all, of these cases of vanishing happen at the same time.

First, suppose that $x = c$, (c being some quantity between a and b) makes $f(x)$ vanish, without making any of the derived functions vanish; then the result of substituting

$$c + h \text{ for } x \text{ in } f(x) \text{ and } f'(x), \text{ is}$$
$$h\,.f'(c) \text{ and } f'(c)$$

(supposing h so small that the signs of the whole of the two series which express $f(c+h)$ and $f'(c+h)$ depend upon those of their first terms, and writing down only the first terms) which have different or the same signs according as h is $-$ or $+$; therefore, in passing from $c-h$ to $c+h$ through a root of the equation, a change of signs is lost, but none gained*.

Secondly, suppose that $x=c$ makes one of the derived functions, $f^m(x)$, vanish, without making any other of the derived functions or $f(x)$ vanish; then the result of substituting $c+h$ for x in

$$f^{m-1}(x),\ f^m(x),\ f^{m+1}(x),$$

(these being the only terms which it is necessary to examine) is

$$f^{m-1}(c),\ h.f^{m+1}(c),\ f^{m+1}(c).$$

If then the extreme terms have the same sign, there will be two changes when h is negative, and two continuations when h is positive; if the extreme terms have contrary signs, there will be one change, and one only, whether h be negative or positive; therefore, in passing from $c-h$ to $c+h$ through a value which makes one of the derived functions vanish, either two changes or none will be lost, but none ever gained.

Thirdly, suppose that $x=c$ makes r consecutive derived functions vanish, without making any other derived function or $f(x)$ vanish; then the result of the substitution of $c+h$ for x in the series

$$f^{m-r}(x),\ f^{m-r+1}(x), \dots f^{m-1}(x),\ f^m(x),\ f^{m+1}(x),$$

(these being the only terms necessary to be examined) is

$$f^{m-r}(c),\ \frac{h^r}{\lfloor r}f^{m+1}(c),\ \dots,\ \frac{h^2}{\lfloor 2}f^{m+1}(c),\ \frac{h}{1}f^{m+1}(c),\ f^{m+1}(c).$$

* It is unnecessary to attend to the other terms of the series of derived functions, because h is supposed so small that not one of them vanishes by the substitution of any quantity between $c-h$ and $c+h$; and therefore each has the same sign for $c-h$ as for $c+h$.

If then the extreme terms have the same sign, there will be r or $r+1$ changes, (according as r is even or odd) when h is negative, and no change when h is positive; if the extreme terms have contrary signs, there will be r or $r+1$ changes (according as r is odd or even) when h is negative, and one change when h is positive; therefore, in passing from $c-h$ to $c+h$ through a value which makes r consecutive derived functions vanish, r or $r \pm 1$ changes are lost (according as r is even or odd) but none ever gained.

Fourthly, suppose the vanishing group to consist of $f(x)$ and the first $r-1$ derived functions {which corresponds to r roots $= c$ in $f(x)=0$}; then the result of the substitution of $c+h$ for x in $f(x)$, $f'(x)$, ... $f^{r-1}(x)$, $f^r(x)$, is

$$\frac{h^r}{\lfloor r} f^r(c),\ \frac{h^{r-1}}{\lfloor r-1} f^r(c), \ldots \frac{h}{1} f^r(c), f^r(c),$$

in which there are r changes when h is negative, and none when h is positive; therefore, in passing through a root which occurs r times in the equation, r changes are lost, but none gained.

Lastly, suppose the substitution of $x=c$ to produce several, or all of the above cases at the same time; then because the conclusions respecting the effect of the passage through c upon the series of signs in one part of the series of derived functions, are not at all influenced by what happens, in consequence the same passage, at another distinct part of the series, by what has been proved several changes will be lost, but none ever gained.

Since then, in substituting gradually ascending values from a to b, an even number of changes of signs, if any, is lost for every passage through a quantity, not a root of $f(x)=0$, which makes one or more of the derived functions vanish; and invariably one for every passage through a root of $f(x)=0$; but none under any circumstances gained; it follows that the number of roots of $f(x)=0$, which lie between a and b, cannot be greater than the excess of

the number of changes given by $x=a$, above that given by $x=b$; and that when it falls short of that excess, it will be by some even number.

109. Hence if the limits, a and b, be $-\infty$ and $+\infty$, or any two numbers, the first of which gives only changes, and the second only continuations; and if in the series formed by $f(x)$ and its derived functions,

$$f(x),\ f'(x),\ f''(x),\ \ldots f^n(x),$$

c be substituted for x and be then made to assume all values between these limits, the series of signs of the results will have the following properties; there will at first be n changes of sign, and at last no change, but n continuations; these changes disappear gradually as c increases, and when once lost can never be recovered; one change disappears every time c passes through a real unequal root of $f(x)=0$; r changes disappear every time c passes through a root which occurs r times in $f(x)=0$; either two or none of the changes disappear every time one only of the derived functions vanishes, without $f(x)$ vanishing at the same time; an even number p of changes disappears, every time an even group of p terms {not including the first, $f(x)$} vanishes; and an even number $q\pm 1$ of changes disappears, every time an odd group of q terms {not including the first, $f(x)$} vanishes. Also if a value causes $f(x)$ and the first $r-1$ derived functions to vanish, and an even group of p terms in one part of the series, and an odd group of q terms in another part, to vanish at the same time; the number of changes lost in passing through that value, will be $r+p+q\pm 1$.

110. Hence if $f(x)=0$ have all its roots real, no value of x can make any of the derived functions vanish, and thereby exterminate changes of signs, without at the same time making $f(x)$ vanish; for if it could, since those changes can never be restored, and since a change must disappear for every passage through a real root, the total number of

changes lost would surpass n, which is absurd. Whenever, therefore, changes disappear between values of x which do not include a root of $f(x)=0$, there is, corresponding to that occurrence, an equal number of imaginary roots of $f(x)=0$. Hence if $x=c$ produces a zero between two similar signs, or if it produces an even number p of consecutive zeros either between similar or contrary signs, there will be, respectively, two, or p, imaginary roots corresponding; or if it produces an odd number q of consecutive zeros, there will be $q \pm 1$ imaginary roots corresponding, according as they stand between similar or contrary signs; c of course not being a root of $f(x)=0$.

Obs. Since the derivatives which follow any one, $f^r(x)$, may be supposed to arise originally from it, it is manifest that the same conclusions respecting the roots of $f^r(x)=0$ may be drawn from observing the part of the series of derivatives

$$f^r(x),\ f^{r+1}(x),\ \ldots f^n(x),$$

as were drawn respecting the root of $f(x)=0$ from the whole series.

111. Hence we can shew that Des Cartes' Rule of Signs is included in Fourier's Theorem as a particular case.

When in the series formed by $f(x)$ and its derived functions, we put $x=-\infty$, there are n changes; and when we put $x=0$, the signs of the series become the same as those of the coefficients

$$p_n,\ p_{n-1},\ \ldots\ p_1,\ 1\ ;$$

let the number of changes in this series of coefficients $=k$, and therefore the number of continuations (supposing the equation complete) $=n-k$; also if we make $x=+\infty$, the signs are all positive, and the number of changes $=0$. Hence between $x=-\infty$ and $x=0$, the number of changes lost is $n-k$; therefore in a complete equation there cannot be more than $n-k$ negative roots, i. e. than the number of continuations in the series of coefficients; also between $x=0$ and

$x=\infty$, the number of changes lost is k, whether the equation be complete or incomplete; hence in any equation there cannot be more positive roots than k, i.e. than the number of changes in the series of coefficients; if there be fewer, the defect will be some even number, indicating a like number of imaginary roots; which is *Des Cartes'* rule of signs.



112. *Fourier's* theorem may also be presented under the following form; under which by some writers it is called the theorem of *Budan*.

If an equation have m real roots between a and b, then the equation whose roots are those of the proposed, each diminished by a, has at least $m+r$ more changes of signs than the equation whose roots are those of the proposed, each diminished by b; where r denotes zero or some even number.

The transformed equations would be

$$f(y+a)=0,\ f(y+b)=0;$$

and if these were arranged according to ascending powers of y, the coefficients would be the values assumed by $f(x)$, $f'(x)$, &c., when a and b are respectively written for x. Therefore, whatever number of changes of signs is lost in the series $f(x)$, $f'(x)$, &c., in passing from a to b, the same is lost in passing from one transformed equation to the other; but the series for a has $m+r$ more changes than that for b, therefore $f(y+a)=0$ has $m+r$ more changes than $f(y+b)=0$, where r is zero or some even number.

113. To apply this method to find the intervals in which the roots of $f(x)=0$ are to be sought, we must substitute successively for x, in the series formed by $f(x)$ and its derivatives, the numbers

$$-\alpha, \ldots -10, -1, 0, 1, 10, \ldots, +\beta \ldots\ldots\ldots (1),$$

($-\alpha$ and $+\beta$ being the least negative, and least positive number, which give, respectively, only changes and continuations) and observe the number of changes of sign in each result.

Let h and k be the numbers of changes of sign when any two consecutive terms in series (1), a and b, are respectively written for x; therefore $h - k$ is the number of real roots that may lie between a and b; if this equals zero, $f(x) = 0$ has no real root between a and b, and the interval is excluded; if $h - k = 1$, or any odd number, there is at least one real root between a and b; if $h - k = 2$, or any even number, there may be two, or some even number, or none; the latter case will happen when, as explained above (Art. 110), some number between a and b makes two or some even number of changes vanish, without satisfying $f(x) = 0$. Similarly, we must examine all the other partial intervals; and when two or more roots are indicated as lying in any interval, their nature must be determined by a succeeding proposition.

The two former of the following examples are extracted from *Fourier's* work.

Ex. 1. $f(x) = x^5 - 3x^4 - 24x^3 + 95x^2 - 46x - 101 = 0$,

$$f'(x) = 5x^4 - 12x^3 - 72x^2 + 190x - 46,$$
$$f''(x) = 20x^3 - 36x^2 - 144x + 190,$$
$$f'''(x) = 60x^2 - 72x - 144,$$
$$f^{iv}(x) = 120x - 72,$$
$$f^{v}(x) = 120.$$

Hence we have the following series of signs resulting from the substitutions of -10, -1, 0, &c., for x in the series of quantities

	f	f'	f''	f'''	f^{iv}	f^{v}
(-10)	•	+	−	+	−	+
(-1)	+	−	+	−	−	+
(0)	−	−	+	−	−	+
(1)	−	+	+	−	+	+
(10)	+	+	+	+	+	+

Hence all the roots lie between -10 and $+10$, because five changes have disappeared; one root lies in each of the

intervals + 10 to − 1, and − 1 to 0, because in each of them a single change is lost; no root lies between 0 and 1 because no change is lost between those limits; and three roots may be sought between 1 and 10 (because three changes have disappeared), one of which is certainly real; it is doubtful whether the other two are real or imaginary.

OBS. When any value c of x, makes one of the derived functions, $f^m(x)$, vanish, we may substitute $c \pm h$ instead of c, h being indefinitely small; then all the other functions will have the same sign as when $x = c$; and the sign of $f^m(c \pm h)$ will depend upon that of $\pm hf^{m+1}(c)$; i. e. it will be the same or contrary to that of the following derivative, $f^{m+1}(c)$, according as h is positive or negative, or according as we substitute a quantity a little greater or a little less than the value which makes $f^m(x)$ vanish. The use of this remark will be seen in the following example.

Ex. 2. $f(x) = x^4 - 4x^3 - 3x + 23 = 0$,

$f'(x) = 4x^3 - 12x^2 - 3$,

$f''(x) = 12x^2 - 24x$,

$f'''(x) = 24x - 24$,

$f^{iv}(x) = 24$.

	f	f'	f''	f'''	f^{iv}
$x = 0$	+	−	0	−	+
$x = 0 \mp h$,	+	−	±	−	+
$x = 1$	+	−	−	0	+
$x = 1 \mp h$,	+	−	−	∓	+
$x = 10$	+	+	+	+	+

Every value less than 0 gives results alternately + and −, therefore there is no real negative root; for $x = 0$, we have a result zero placed between two similar signs, and therefore corresponding to it there is a pair of imaginary roots. There is no root between 0 and 1, but there may be two roots between 1 and 10.

Ex. 3. $f(x) = x^6 - 6x^5 + 40x^3 + 60x^2 - x - 1 = 0$.

Here there is no root < -1; there is one, and there may be three, between -1 and 0; there is one root between 0 and 1; and there may be two roots between 2 and 3.

114. The above process will determine the intervals in which the roots are to be sought, but not always their nature; when an even number of roots is indicated, they may all turn out to be impossible. The series of magnitudes, between $-\infty$ and $+\infty$, to be substituted for x in the derived functions, has been divided into intervals of two sorts, each contained by assigned limits, a and b. The first sort of interval is one within which no root is comprehended; i.e. the limits of which, give the same number of changes of signs in the series of derived functions. The second sort is one within which roots may lie; i.e. where the number of changes resulting from the substitution of b, is less than the number resulting from the substitution of a, in the series of derived functions. This second sort of interval has two subdivisions, viz. cases where the indicated roots do really exist, and others where they are imaginary. When we have ascertained that a certain number of roots may lie between a and b, we may substitute c (a quantity between a and b) in the series of derived functions, and if any changes disappear, our interval is broken into two others; if no changes disappear, we may increase or diminish c, and make a second substitution, and it may still happen that no change is lost; and so on continually; and we may be left after all in a state of uncertainty, whether the separation of the roots is impossible because they are imaginary, or only retarded because their difference is extremely small.

Hence when we know that two limits may include a certain number of roots, we must have a special rule for determining whether they are possible or impossible; this has been given by *Fourier* in the two following propositions; in proving which, we assume that the development of $f(x+h)$

in Art. 27 may be put under the following forms, so as to exhibit the remainder of the series, when we take only one, two, &c. terms (see Art. 121);

$$f(x+h) = f(x) + hf'(\lambda),$$

$$f(x+h) = f(x) + hf'(x) + \tfrac{1}{2}h^2 f''(\mu),$$

and so on, where λ, μ, &c., are quantities certainly situated between x and $x+h$, but of which the exact values are unknown, and for our purpose are unnecessary.

115. Having given that between two limits a and b, $f''(x) = 0$ has no root at all, $f'(x) = 0$ one root and no more, and that $f(x) = 0$ may have either two roots or none, to discover whether these roots exist or not.

By what has already been proved, the series of signs resulting from the substitution of a in the series of quantities

$$f(x),\ f'(x),\ f''(x),\ \dots f^n(x),$$

will present two more changes than the series resulting from the substitution of b; also, if we leave out the first term, there will be one more change for a than for b; and if we leave out the first two terms, there will be exactly the same number of changes for a as for b. Therefore $f(x)$ and $f''(x)$ will be both constantly positive, or constantly negative, for a and b, and for all intermediate values; and $f'(x)$ will have a sign different from that of $f(x)$ and $f''(x)$ when $x = a$, and the same as that of $f(x)$ and $f''(x)$ when $x = b$.

The two roots of $f(x) = 0$, indicated as lying between a and b, will be real or imaginary, according as it is, or is not, possible to find a quantity c, between a and b, such that $f(c)$ shall have a sign contrary to that which is common to $f(a)$ and $f(b)$.

Let therefore, if possible,

$$c = a + h = b - k$$

be a quantity between a and b, such that

$$\frac{f(c)}{f(a)} = \text{neg.} \quad \frac{f(c)}{f(b)} = \text{neg.};$$

or, expanding so that the terms of the second order may include the remainder of each series, and denoting by λ, μ, quantities intermediate to a and b,

$$1 + h \cdot \frac{f'(a)}{f(a)} + \frac{h^2}{2} \cdot \frac{f''(\lambda)}{f(a)} = \text{neg.}$$

$$1 - k \cdot \frac{f'(b)}{f(b)} + \frac{k^2}{2} \cdot \frac{f''(\mu)}{f(b)} = \text{neg.}$$

Or, since under the given conditions the last fraction in each line must be positive, and also

$$\frac{f'(a)}{f(a)} = \text{neg.}, \quad \frac{f'(b)}{f(b)} = \text{pos.},$$

we must have

$$\frac{f(a)}{f'(a)} + h = \text{pos.} \quad \frac{f(b)}{f'(b)} - k = \text{neg.};$$

$$\therefore \quad \frac{f(a)}{f'(a)} - \frac{f(b)}{f'(b)} + h + k = \text{pos.}$$

$$\text{or } h + k = b - a > \frac{f(b)}{f'(b)} - \frac{f(a)}{f'(a)}.$$

If then this condition can be satisfied, a quantity c, between a and b, may exist so as to make $f(c)$ of a sign contrary to $f(a)$ and $f(b)$; and if it can be found, the indicated roots are real and are separated: but if the condition is not satisfied, that is, if the difference of the limits be equal to, or less than, the sum of the fractions

$$\frac{f(a)}{f'(a)}, \quad \frac{f(b)}{f'(b)},$$

taken without regard to sign, no such value of c exists, and the indicated roots are imaginary.

It is manifest that if any three consecutive derivatives,

$$f^r(x),\ f^{r+1}(x),\ f^{r+2}(x),$$

satisfy the prescribed conditions for a given interval, the same process will determine the nature of the pair of roots of $f'(x)=0$ indicated in that interval; and whatever number of impossible roots $f'(x)=0$ may have, $f(x)=0$ has at least as many (Art. 53).

116. When the above condition is satisfied, we must substitute a quantity c between a and b in $f(x)$; if $f(c)$ has a sign contrary to the common sign of $f(a)$ and $f(b)$, the separation is effected; if not, we infer that the limits are not sufficiently close to determine the nature of the indicated roots by a single process. In the latter case, $f'(c)$ necessarily differs in sign from one or the other of $f'(a)$, $f'(b)$; choosing, then, that limit which makes $f'(x)$ have a contrary sign from $f'(c)$, we must with it and c repeat exactly the same process; and we are certain at last to discover either that no roots exist in the interval, or to separate them if they do.

Ex. $\quad x^5-3x^4-24x^3+95x^2-46x-101=0.$

	f	f'	f''	f'''	f^{iv}	f^{v}
(2)	−	+	−	−	+	+
	2	1	0			
(3)	−	−	−	+	+	+.

Here, since there are two more changes for $x=2$, than for $x=3$; one more, omitting the first term; and the same number, omitting the two first terms; the equation may have two roots between 2 and 3, and the conditions respecting the roots of $f'(x)=0$, $f''(x)=0$ are satisfied; and since for the two limits, the fraction

$$\frac{f(x)}{f'(x)} \text{ becomes } \frac{7}{10} \text{ and } \frac{32}{43},$$

the sum of which is greater than the difference, 1, of the limits; therefore the two indicated roots are imaginary.

117. In the next proposition, it will be necessary, for any proposed interval, to know the number of roots which each derivative, when formed into an equation, may have in that interval. The best practical way of doing this, is, in the two series of signs produced by the two limits, to write over each sign the number of changes presented by the series commencing with that sign and going to the end of the series; and then to take the difference between each number in the upper line and the corresponding one in the lower. Applying the process to the foregoing example, we have

	3	2	1	1	0	0
(2)	−	+	−	−	+	+
	2	1	0	1	0	0
(3)	−	−	−	+	+	+
	1	1	1	0	0	0

where the series of indices 2, 1, 0, 1, 0, 0, mark the number of roots which the equations

$$f(x) = 0, \; f'(x) = 0, \; f''(x) = 0, \; \&c.,$$

may have, between the limits 2 and 3. Also, we observe that in this series (and indeed in every case, if we consider the way in which they are formed,) any index has immediately adjacent to it, either the same, or one differing from it by the addition of ± 1.

118. When any number of roots of $f(x) = 0$ are indicated as lying between a and b, this interval may always be broken up into others, in which such of the roots as are real are situated singly.

From observing the number of changes lost in the series formed by $f(x)$ and all its derivatives, and also in the series formed by each of the derivatives and all those which follow it, in passing from a to b, let the number of roots which $f(x) = 0$ may have, or which the derivatives taken in order when formed into equations may have, between those limits, be determined; and let them be δ, δ', δ'', &c. Now suppose

that in the series (where each function is accompanied by its index, i.e. the number of roots which, when formed into an equation, it may have between a and b)

$$\begin{array}{cccccccc} f(x) & f'(x) & f''(x) & \ldots & f^{r-1}(x) & f^{r}(x) & f^{r+1}(x), & \ldots \\ \delta & \delta' & \delta'' & & 2 & 1 & \epsilon & \end{array}$$

$f^r(x)$ is the first whose index is 1; then the preceding function has 2 for its index, for it cannot have 0, otherwise, since the first index is not zero, there would be some function before $f^r(x)$ having 1 for its index. Now if ϵ be not zero, since $f^r(x) = 0$, $f^{r+1}(x) = 0$, cannot have a common root, two new limits a', b', may be found within the former, intercepting the root of $f^r(x) = 0$, but excluding every root of $f^{r+1}(x) = 0$. Hence the interval a, b, will be broken up into the three aa', $a'b'$, $b'b$, the first and third of which give for $f^r(x)$ an index zero, and therefore an index 1 to some preceding function, and the second $a'b'$ will either make some preceding function have an index 1, or will allow $f^r(x)$ still to be the first function whose index is unity for that interval, the indices of $f^{r-1}(x)$ and $f^{r+1}(x)$ being 2 and 0.

Suppose the latter to be the case; then, by Art. 115, we may find whether $f^{r-1}(x) = 0$ has two real roots or none between a' and b'; if there are two real roots, then taking a quantity c' between them, the interval $a'b'$ is divided into the two $a'c'$ and $c'b'$, each of which makes $f^{r-1}(x)$, or some preceding function, have an index 1; but if the two roots of $f^{r-1}(x) = 0$, indicated as lying between a' and b', are imaginary, since every quantity intermediate to a' and b' will make $f^{r-1}(x)$ and $f^{r+1}(x)$ have the same sign, therefore in passing from a' to b' through the root of $f^r(x) = 0$, since the adjacent functions have the same sign, two changes will be lost. Hence we may diminish the indices of all the preceding functions by 2, and proceed, relative to the interval $a'b'$, with that function preceding $f^r(x)$ which first has 1 for its index. Hence the proposed interval is replaced by partial intervals, in each of which the separation of the included

roots is more nearly effected than in the original interval; and by proceeding with the partial intervals in the same manner as we did for a, b, we shall at last find only intervals in which the index of $f(x)$ is either 0 or 1; and the separation of the roots of $f(x)=0$ which lie between a and b, will be completely effected.

Ex. $f(x)=x^4-x^3+4x^2+x-4=0$,

	f	f'	f''	f'''	f^{iv}
(-10)	+	−	+	−	+
(-1)	+	−	+	−	+
(0)	−	+	+	−	+
	3	2	2	1	0
(1)	+	+	+	+	+

There is no root between -10 and -1, and one root between -1 and 0, also three are indicated between 0 and 1; but, forming the series of indices for that interval, we see that $f''(x)=0$ is the first equation to which the criterion can be applied; also $\dfrac{f''(x)}{f'''(x)}$ becomes $\dfrac{6x^2-3x+4}{12x-3}$ which, for $x=0$, becomes $-\dfrac{4}{3}$, and this neglecting the sign is greater than 1, the difference of the limits; therefore the roots are imaginary, and consequently there is only one root of the proposed equation between 0 and 1.

GEOMETRICAL ILLUSTRATION OF FOURIER'S METHOD OF SEPARATING THE ROOTS.

119. The criterion of the reality of two indicated roots in any interval may be readily deduced from geometrical considerations.

Let $y=f(x)$ be the equation to a parabolic curve; then the portion of it between $x=a$, $x=b$, (supposing these limits to satisfy all the prescribed conditions,) must have the shape PCQ (Fig. 2), O being the origin, ONM the axis of x, PN,

QM, the ordinates of its extremities having the same sign, C the single point where the tangent is parallel to the axis, and the curve through the extent PCQ being convex to the axis of x, because for that interval $f(x)$ and $f''(x)$ have the same sign. But if $O'N'M'$, a line parallel to ONM and cutting the curve in two points, be the axis of x, the curve will have the ordinates of its extremities of the same sign, and will have its tangent parallel to the axis of x at one single point, and $f(x), f''(x)$ will have the same sign for all points between P and Q; hence, for any thing that yet appears, this construction will represent the function $f(x)$ between $x = a$ and $x = b$, just as well as the former; but it is manifest that when $f(x) = 0$ has two roots between a and b, there will be two points of intersection with the axis of x, and the second is the true construction; and the former belongs to the case where there is no point of intersection, and where the abscissæ of the points of intersection, that is, the roots of $f(x) = 0$, are imaginary. If we knew the exact value, c, of OR, we might substitute it in $f(x)$, and if the sign of the result was different from that of $f(a)$ and $f(b)$, then $f(c)$ would be represented by $R'C$, and we should be certain that there were two points of intersection; if the same, $f(c)$ would be represented by RC, and there would be no point of intersection. But if we can only find an approximate value of c, and the sign of $f(c)$ is the same as that of $f(a)$ and $f(b)$, we are uncertain whether the points of intersection are imaginary, or so near to one another that our approximate foot of the least ordinate does not fall between them.

Now in the case of real roots, that is, when $O'N'M'$ is the axis of x, and there are two points of intersection, if tangents Pt', Qs' be drawn at P, Q, it is manifest, that however near to one another the roots are, and however close the limits are to the roots, $N'M'$ must exceed $N't' + M's'$, or $b - a$ must exceed $\frac{f(b)}{f'(b)} - \frac{f(a)}{f'(a)}$; if therefore we find either

$\frac{f(b)}{f'(b)}$, or $-\frac{f(a)}{f'(a)}$, or their sum, greater than $b-a$, we know that the roots cannot be possible, and may pronounce them impossible.

But when we find the difference of the limits greater than the sum of the subtangents, we cannot conclude that the roots are possible; for this condition is satisfied not only by the axis $N'M'$ but also by NM, as long as the tangents Pt, Qs, do not intersect between the curve and the axis.

In the latter case, we must substitute a quantity d between a and b for x, then if $f(d)$ have a different sign from $f(a)$ and $f(b)$, the two indicated roots are real, and their separation is effected; if not, $f'(d)$ will have the same sign either as $f'(a)$ or $f'(b)$; let it be the former, then no root can lie between a and d; and we must now apply the criterion of the subtangents to the new and closer interval from d to b.

120. To avoid the risk of trying to separate two roots that are actually equal to one another, it will be often requisite to ascertain directly whether

$$f(x) = p_0x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n = 0 \ldots\ldots (1)$$

admits of a pair of equal roots; and the labour of doing so may be shortened by the following considerations. If (1) has a single pair of equal roots, they must be commensurable; for in that case $f(x)$ and $f'(x)$ admit of a common divisor $x-c$ which, put equal to zero, will give a rational value for the root that occurs twice. If $p_0 = 1$, the equal root c must be an integer (Art. 65), and p_{n-1}, p_n must be divisible respectively by c, c^2; if p_0 be not unity, the equal root must be a fraction $a \div b$, and p_{n-1}, p_n, p_1, p_0 must be divisible respectively by a, a^2, b, b^2 (Art. 32). In both cases, if a suspected equal root be not excluded by these conditions, we must try by substitution whether it satisfies $f(x) = 0$, $f'(x) = 0$.

SECTION VII.

ON THE METHODS OF FINDING APPROXIMATE VALUES OF THE REAL INCOMMENSURABLE ROOTS OF EQUATIONS.

---

121. WHEN all the commensurable roots of an equation have been found, and all the incommensurable roots separated by the methods explained in the foregoing sections, the next step towards the solution of the equation is to find approximate values of the incommensurable roots; and to this we shall now direct our attention.

It will however be necessary previously to prove certain properties of the polynomial $f(x)$, which forms the first member of the equation.

Since $f(x+h) - f(x) = f'(x)\,h + f''(x)\,\frac{h^2}{2} + \ldots + h^n$,

and as long as x is finite, none of the quantities $f'(x)$, $f''(x)$, &c., being integral functions, can become infinite, therefore by taking h sufficiently small we may make the second member as small as ever we please; consequently if x increase continuously by insensible degrees between two limits a and b, $f(x)$ will also vary continuously by insensible degrees between the same limits; and will go on increasing as long as $f'(x)$ continues positive; and when $f'(x)$ is negative, it will go on diminishing.

Again, since

$$\frac{f(x+h) - f(x)}{h} = f'(x) + f''(x)\,\frac{h}{2} + \ldots + h^{n-1},$$

and since by diminishing h we can make

$$f''(x)\frac{h}{2}+\ldots+h^{n-1}$$

as near zero as ever we please, or always intermediate in value to $+e$ and $-e$, where e is as near zero as ever we please; by taking h sufficiently small, we shall always have

$$\frac{f(x+h)-f(x)}{h}>f'(x)-e<f'(x)+e;$$

if therefore x be always taken between a and b, and if A, B, denote the least and greatest values which $f'(x)$ can assume between those limits, *à fortiori*, the following inequality may be satisfied,

$$f(x+h)-f(x)>h(A-e)<h(B+e).$$

Suppose now that, between the limits a and b, are interposed a series of ascending values of x, α_1, α_2, ... α_n so near to one another that the above inequality may be always satisfied, when we take one of those values for x and the following one for $x+h$; then

$$f(\alpha_1)-f(a)>(\alpha_1-a)(A-e)<(\alpha_1-a)(B+e)$$
$$f(\alpha_2)-f(\alpha_1)>(\alpha_2-\alpha_1)(A-e)<(\alpha_2-\alpha_1)(B+e)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f(b)-f(\alpha_n)>(b-\alpha_n)(A-e)<(b-\alpha_n)(B+e);$$

therefore, adding,

$$f(b)-f(a)>(b-a)(A-e)<(b-a)(B+e);$$

or, since this is true however small e is,

$$f(b)-f(a)>(b-a)A<(b-a)B.$$

But as x changes by insensible degrees from a to b, $f'(x)$ will change by insensible degrees, and will assume all values between A and B, these being the least and greatest values which it can have in that interval. Therefore every quantity

between A and B will be a value of $f'(x)$ corresponding to some value of x between a and b. Suppose therefore

$$\frac{f(b)-f(a)}{b-a},$$

which we have shewn to lie between A and B, to be equal to the value assumed by $f'(x)$ when $x=\lambda$; then

$$f(b)=f(a)+(b-a)f'(\lambda),$$

where λ is some quantity lying between a and b.

NEWTON'S METHOD OF APPROXIMATION.

122. When we know an approximate value of a root, we may easily obtain other values of it, more and more exact, by a method invented by *Newton*, which rapidly attains its object. We shall give this method, first in the form in which it was proposed by its author, and afterwards with the conditions which *Fourier* has shewn to be necessary for its complete success.

Let $f(x)=0$ be an equation having a root c between a and b, the difference of these limits, $b-a$, being a small fraction whose square may be neglected in the process of approximation.

Let c_1, a quantity between a and b, be assumed as the first approximation to c, then $c=c_1+h$, where h is very small;

$$\therefore f(c_1+h)=0,$$

$$\text{or } f(c_1)+f'(c_1)\,h+f''(c_1)\,\frac{h^2}{2}+\ldots+h^n=0.$$

Now since h is very small, h^2, h^3, &c., are very small compared with h; also none of the quantities $f''(c_1)$, $f'''(c_1)$, &c., can become very great, since they result from substituting a finite value in integral functions of x; therefore, provided $f'(c_1)$ be not very small (that is, provided $f'(x)=0$ have no root nearly equal to c_1 or to c, and consequently $f(x)=0$ no other root nearly equal to c besides the one we are

approximating to) all the terms in the series after the first two may be neglected in comparison with them; and we have, to determine h_1 the resulting approximate value of h, the equation

$$f(c_1) + h_1 f'(c_1) = 0;$$

$$\therefore\ h_1 = -\frac{f(c_1)}{f'(c_1)} = -\left\{\frac{f(x)}{f'(x)}\right\}_{x=c_1},$$

and the second approximation is

$$c_2 = c_1 + h_1 = c_1 - \left\{\frac{f(x)}{f'(x)}\right\}_{x=c_1}.$$

Similarly, starting from c_2 instead of c_1, the third approximate value will be

$$c_3 = c_2 - \left\{\frac{f(x)}{f'(x)}\right\}_{x=c_2},$$

and so on; and if we can be certain that each new value is nearer to the truth than the preceding, there is no limit to the accuracy which may be obtained.

Ex. 1. $x^3 - 2x - 5 = 0.$

Here, one root lies between 2 and 3, and the equation can have only one positive root; also, upon narrowing the limits, we find that $x = 2$ gives a negative, and $x = 2{\cdot}2$ a positive result, therefore 2·1 differs from the root by a quantity less than 0·1, and we may assume $c_1 = 2{\cdot}1$. Hence

$$c_2 = 2{\cdot}1 - \left(\frac{x^3 - 2x - 5}{3x^2 - 2}\right)_{x=2{\cdot}1} = 2{\cdot}1 - \frac{0{\cdot}061}{11{\cdot}23},$$

$$\text{or } c_2 = 2{\cdot}1 - 0{\cdot}0054 = 2{\cdot}0946.$$

Similarly,

$$c_3 = 2{\cdot}09455149.$$

Ex. 2. $x^3 - 7x - 7 = 0.$

There is only one positive root, lying between 3 and 3·1; and it equals 3·048917339.

Obs. To guard against over correction, that is, against applying such a correction to an approximate value, as shall

make the new value differ more from the root by excess than the original approximate value did by defect, or *vice versâ*, we must be certain that each new value is nearer to the truth than the preceding; this gives rise to the following conditions, first noticed by *Fourier*.

123. For the complete success of *Newton's* method of approximation, the following conditions are necessary.

(1) The limits between which the required root is known to lie must be so close, that no other root of $f(x)=0$, and no root of $f'(x)=0$, or $f''(x)=0$, lies between them.

(2) The approximation must be begun and continued from that limit which makes $f(x)$ and $f''(x)$ have the same sign.

Let c be a root of $f(x)=0$ which lies between a and b, $a<b$, c_1 the first approximate value, and h the whole correction, so that $c=c_1+h$;

$$\text{then } f(c_1+h)=0, \quad \text{or } f(c_1)+hf'(\lambda)=0,$$

λ being some quantity between c_1 and c, (Art. 121).

Therefore, supposing $\lambda=c_1$, which amounts to neglecting all powers of h above the first, and requires that $f(x)=0$ have no root besides c in that interval, and calling the resulting approximate value of h, h_1, we have

$$f(c_1)+h_1 f'(c_1)=0.$$

Now the true value is $c=c_1+h$,

the 1st approximate value is c_1 with error h,

the 2nd approximate value is $c_2=c_1+h_1$ with error $h-h_1$, which (neglecting signs) must be less than h,

i.e. $h^2-(h-h_1)^2$ must be positive, or $2hh_1-h_1^2=+$,

$$\text{or } \frac{h}{h_1}-\tfrac{1}{2}=+, \quad \text{or } \frac{f'(c_1)}{f'(\lambda)}-\tfrac{1}{2}=+;$$

which condition (since λ is an indeterminate quantity between c_1 and c, or between a and b) cannot in all cases be

secured unless $f'(x)$ be incapable of changing its sign between a and b; i.e. unless $f'(x)=0$ have no root between a and b.

Moreover, we must have $\frac{f'(c_1)}{f'(\lambda)} > \frac{1}{2}$, or > 1.

Now if $f''(x)$ preserve an invariable sign between a and b, i.e. if $f''(x)=0$ have no root in that interval, then $f'(x)$ will increase or diminish continually from a to b; therefore c_1 must be taken equal to that limit which gives $f'(x)$ its greatest numerical value without regard to sign.

First, let $f'(x)$, $f''(x)$, have the same sign from a to b; then $f'(x)$ increases continually in that interval; therefore we must have $c_1 = b$, or we must begin from the greater limit. But $f(b)$ has the same sign as $f(c+h) = f(c) + hf'(c) = hf'(c)$, or as $f'(c)$; therefore we must have c_1 equal to that limit which makes $f(x)$ and $f''(x)$ have the same sign.

Secondly, let $f'(x)$, $f''(x)$, have contrary signs from a to b; then $f'(x)$ diminishes continually in that interval; therefore we must have $c_1 = a$, or we must begin from the lesser limit. But $f(a)$ has the same sign as $f(c-h) = f(c) - hf'(c) = -hf'(c)$, or as $-f'(c)$; therefore in this case, equally as in the former, we must have c_1 equal to that limit which makes $f(x)$ and $f''(x)$ have the same sign.

These conditions being fulfilled, we have

$$\frac{f'(c_1)}{f'(\lambda)} - 1 = +, \text{ or } \frac{h-h_1}{h_1} = +,$$

$$\text{or } \frac{c-c_2}{c_2-c_1} = +;$$

therefore c_2 lies between c and c_1; hence the new limit c_2 fulfils the requisite conditions, and we may with certainty from it continue the approximation.

124. To estimate the rapidity of the approximation, we have

error in 1st approximate value c_1, $= h$,
error in 2nd approximate value c_2, $= h - h_1$.

But $$f(c_1)+hf'(c_1)+\tfrac{1}{2}h^2f''(\mu)=0,$$
$$f(c_1)+h_1f'(c_1)=0;$$
$$\therefore\ (h-h_1)f'(c_1)+\tfrac{1}{2}h^2f''(\mu)=0,$$
$$\text{or } h-h_1=-\tfrac{1}{2}h^2\frac{f''(\mu)}{f'(c_1)}.$$

Let the greatest value which $f''(x)$ can assume between a and b (which will be either $f''(a)$ or $f''(b)$, if $f'''(x)=0$ have no root in the interval) be divided by the least value of $2f'(x)$ in that interval which will be either $2f'(a)$ or $2f'(b)$, and let the quotient be denoted by C; then, neglecting signs,

$$h-h_1<h^2C;$$

hence if the first error h in c_1 be a small decimal, the error $h-h_1$ with which c_2 is affected (since C will not, except in particular cases, be very large) will be very small compared with h; and if the quantity C be less than unity, the number of exact decimals in the result will be doubled by each successive operation. The quantity C, when thus computed for a given interval, preserves the same value throughout the operations which it may be necessary to make in order to approximate to the value of the root lying in that interval; and as we thus know a limit to the difference between the approximate value already found and the true value, we may always avoid calculating decimals which are inexact, and only obtain those which are necessarily correct.

Ex. $$6x^3-141x+263=0.$$

This equation has two positive roots, one between 2·7 and 2·8, and the other between 2·8 and 2·9. Now $f'(x)$ $=18x^2-141=0$, has a root $=\sqrt{\frac{47}{6}}=2{\cdot}798$ between 2·7 and 2·8, therefore these limits are not sufficiently close; but this root is greater than 2·79; also 2·7 and 2·79 substituted in $f(x)$ gives results with different signs; and 2·7 substituted in $f(x)$ and $f''(x)$ gives results with the same sign; therefore $c_1=2{\cdot}7$.

With regard to the other interval $2\cdot8$, $2\cdot9$, $f'(x)=0$, $f''(x)=0$, have no roots between these limits, and $2\cdot$ makes $f(x)$ and $f''(x)$ have the same sign; therefore $c_1=2\cdot9$; and starting from these values we are certain in each case to get a new value nearer to the truth.

Again, the greatest value which $\dfrac{f''(x)}{f'(2\cdot7)}$ can assume in the interval $2\cdot7$, $2\cdot79$, is nearly equal to 10; hence if h_1, h_2, be consecutive errors, we have $h_2 < \frac{1}{2}(h_1)^2.10$.

The same formula will be found to be true for consecutive errors in the interval $2\cdot8$, $2\cdot9$.

GEOMETRICAL ILLUSTRATION OF NEWTON'S METHOD OF APPROXIMATION.

125. The nature of *Newton's* method of approximation, and the necessity of *Fourier's* limitations, are well illustrated by the following geometrical considerations.

Let $y=f(x)$ be the equation to a parabolic curve, then the portion of it between $x=a$ and $x=b$, (supposing these limits to satisfy all the prescribed conditions,) must have the shape PCQ, (Fig. 1,) O being the origin, OC the axis of x, PN, QM the extreme ordinates having different signs; and there being no point of inflexion and no tangent parallel to the axis in the interval between $x=a$ and $x=b$, since neither $f''(x)=0$, nor $f'(x)=0$ has a root between a and b. Now if QT be a tangent at Q, it is manifest that OT will be intermediate to OC and OM, whatever be the magnitude of CM; but $MT=\dfrac{f(b)}{f'(b)}$ is the correction furnished by *Newton's* method; hence if we start with that end of the arc which is convex towards the axis of x, and therefore from that limit $OM=b$ which makes $f(x)$ and $f''(x)$ have the same sign, we shall get a new limit $OT=b'=b-\dfrac{f(b)}{f'(b)}$, which is certainly

closer than the former and on the same side of the root; and if we repeat the process with b', the next value of the root will be $OT'_{\!*}$, which is still nearer to the truth. But if we commence with that end of the arc which is concave to the axis of x, and therefore from that limit $ON = a$ which makes $f(x)$ and $f''(x)$ have contrary signs, the correction will be $NU = -\dfrac{f(a)}{f'(a)}$; and the new value OU will exceed OC, and may exceed OC by more than ON falls short of OC; so that we cannot be certain that the new limit is cl. er than the former; and if we again correct OU, the result may be still more erroneous.

We may however obtain a new inferior limit by drawing PS parallel to QT, then OS will always lie between ON and OC, and we have $NS = -\dfrac{f(a)}{f'(b)}$, and $OS = a - \dfrac{f(a)}{f'(b)}$. Thus we have two new limits, and as many figures as their values have in common, so many are exact in the approximation.

If the primitive interval were not sufficiently small to exclude all roots of $f'(x) = 0$ and $f''(x) = 0$, then it might happen that the limit b might correspond to a point B situated beyond a point of inflexion R, and the tangent at B might meet the axis at a point remote from C; and if B were situated at the extremity of a maximum ordinate, the result would be still more erroneous.

In connection with these geometrical illustrations of *Newton's* method of approximation, and of *Fourier's* criterion of the reality of two roots at Art. 118, the following remarks may be made. If instead of the equation $f(x) = 0$, we consider the equation $f(x) = y$, and suppose y to assume successive known values, we shall have a system of equations, differing only in their final terms; and the roots of all of them may be exhibited by means of the intersections of the same curve with a system of parallel straight lines. For suppose the equation $f(x) = y$ to represent the curve PCQ (fig. 2) when

referred to ONM as axis of x; then if we draw another axis $O'N'M'$ parallel to the former, and call $NN'=a$, we have $PN'=y'=y-a$, so that relative to the new axis the same curve is represented by the equation $y'+a=f(x)$; and if we suppose $y'=0$, the roots of $f(x)-a=0$, are the abscissæ of the points of intersection $O'A$, $O'B$, &c. If the new axis were drawn so as to touch the curve at C, and $CR=c$, then the equation $f(x)-c=0$ would have a pair of roots $=O'R'$; and if b were taken less than c, so that the axis were situated between C and R, then $f(x)-b=0$ would have a pair of imaginary roots, the curve having receded from the axis without intersecting it. We thus perceive that the slightest alteration in the final term of an equation, may change two real roots lying close together, into a pair of equal roots, or into a pair of imaginary roots conjugate to one another.

126. The following method, known as *Horner's* method, of calculating the real incommensurable roots of a numerical equation, is laborious; but it possesses the advantage of determining with certainty, to as many places of decimals as may be desired, the successive digits in the decimal part of any root known to lie between two consecutive integers. It requires a peculiar mode of forming the equation whose roots shall be those of a proposed equation diminished by a given quantity, which we proceed to explain.

If we wish to diminish the roots of a numerical equation of the n^{th} degree, $X_n=0$, by a given number a, we may, instead of putting $x=y+a$ as in Art. 25 and expanding, employ the following more expeditious method. Dividing X_n by $x-a$, let X_{n-1} be the quotient, and r_1 the remainder which is numerical; again, dividing X_{n-1} by $x-a$, let X_{n-2} be the quotient and r_2 the remainder; and so on through n divisions; then

$$X_n = (x-a)\,X_{n-1}+r_1,$$
$$X_{n-1}=(x-a)\,X_{n-2}+r_2,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$X_1 = (x-a)\,1+r_n;$$

hence by successive substitutions we get the transformed equation

$$X_n = (x-a)^n + r_n (x-a)^{n-1} + \ldots + r_1 = 0.$$

The coefficients $r_1, r_2, \ldots r_n$, which are the remainders after one, two, &c., n repeated divisions of X_n by $x-a$, can be readily found from Art. 6; where it is shewn that when any polynomial $f(x)$ is divided by $x-a$, the coefficient of the first term in the quotient is the same as that of the first term of the polynomial; and the other coefficients and the remainder are formed, one from the other, by multiplying the coefficient of the preceding term by a and adding the product to the coefficient of that term of $f(x)$ which involves the same power of x as the preceding term does; the last quantity that can be so formed being the remainder. Hence if we perform n separate divisions of X_n by $x-a$ by this uniform process, we shall obtain n remainders, which are the coefficients of the transformed equation. The facility of the method will be seen in the following examples; when $a = 1$, the process is merely one of addition.

Ex. 1. To diminish by 4 the roots of the equation

$$2x^4 - 6x^3 - x^2 + 0x + 3 = 0.$$

2	2	7	28,	$115 = r_1$,
	2	10	47,	$216 = r_2$,
		2	18,	$119 = r_3$,
			2,	$26 = r_4$;

$$\therefore\ 2(x-4)^4 + 26(x-4)^3 + 119(x-4)^2 + 216(x-4) + 115 = 0.$$

The second line gives the coefficients of the quotient

$$2x^3 + 2x^2 + 7x + 28,$$

and the remainder 115, after dividing the proposed by $x-4$, which are calculated thus: 2 we know is the coefficient of x^3, and if we multiply it by 4 and add the product to -6, the coefficient of the same power of x in the line above, we get 2 the coefficient of x^2; again, multiplying 2 by 4 and adding the product to the coefficient of x^2 in the line above, we get

7 for the coefficient of x; and so on. In the third line are given the coefficients of the quotient, and the remainder, after dividing $2x^3+2x^2+7x+28$ by $x-4$ (which amounts to performing two successive divisions of the proposed by $x-4$); and they are formed by the same uniform law, of multiplying any one by 4 and adding the product to the coefficient which stands over it in the line above, for the next following coefficient. When the roots are to be diminished by unity, the process is still easier, as no multiplication is requisite in forming the coefficients. Thus if it were required to diminish by unity the roots of the above equation

$$2x^4 - 6x^3 - x^2 + 0x + 3 = 0,$$
$$2 \quad -4 \quad -5 \quad -5, \quad -2 = r_1,$$
$$2 \quad -2 \quad -7, \quad -12 = r_2.$$
$$2 \quad 0, \quad -7 = r_3.$$
$$2, \quad 2 = r_4;$$

$$\therefore\ 2(x-1)^4 + 2(x-1)^3 - 7(x-1)^2 - 12(x-1) - 2 = 0.$$

The former result shews that $x-4$ has no positive value, and this shews that $x-1$ has but one positive value; therefore the proposed has but one root greater than 1, and it is less than 4.

Ex. 2. To diminish by 3 the roots of the equation

$$4x^7 - 6x^6 - 7x^5 + 8x^4 + 7x^3 - 23x^2 - 22x - 5 = 0.$$

The transformed equation, which may be calculated with the same ease as in the preceding example, will be found to be

$$4(x-3)^7 + 78(x-3)^6 + 641(x-3)^5 + 2873(x-3)^4$$
$$+ 7573(x-3)^3 + 11704(x-3)^2$$
$$+ 9722(x-3) + 3232 = 0,$$

and shews that the proposed has no root greater than 3.

It is plain that when all the roots of an equation are possible, this method of transformation combined with *Des Cartes'* Rule of Signs, will afford a ready means of separating

the roots. For suppose the roots to be diminished by some number a, and let the proposed and transformed equation be

$$x^n + p_1 x^{n-1} + \ldots + p_n = 0 \ldots\ldots\ldots\ldots\ldots (1),$$

$$(x-a)^n + r_n (x-a)^{n-1} + \ldots + r_1 = 0 \ldots\ldots\ldots (2);$$

then these equations give as many positive values for x, and for $x-a$, respectively, as each has changes of sign. If they present the same number of changes, there is no positive value of x less than a; if (2) has a certain number less of changes than (1), then x admits of the same number of values between 0 and a. Again, if a second transformed equation, where $b > a$,

$$(x-b)^n + \rho_n (x-b)^{n-1} + \ldots + \rho_1 = 0,$$

present a certain number less of changes than (2), x will admit of the same number of values between a and b. If therefore we deduce in succession the several transformed equations in $x-1$, $x-2$, ... $x-10$, and count the changes lost at each transformation, we shall learn how many roots the proposed has between 0 and 1, 1 and 2, ... 9 and 10.

127. When by the preceding or any other of the methods that have been devised for separating the roots, the equation $f(x) = 0$ is found to have one root, and one only, between a and $a+1$, we may calculate with certainty, to as many places of decimals as may be desired, the successive digits in the decimal part of that root. We must first transform $f(x)$ by the method just explained, so that

$$f(x) = (x-a)^n + r_n (x-a)^{n-1} + \ldots + r_1 = 0,$$

where r_1, r_2, ... r_n are the remainders after 1, 2, &c. n repeated divisions of $f(x)$ by $x-a$; then making $x-a=y$, or $x=a+y$, we get

$$y^n + r_n y^{n-1} + \ldots + r_1 = 0,$$

which has its roots equal to those of $f(x)=0$, each diminished by a, and it has therefore one root, and one only, between 0 and 1. Consequently (Art. 30) the equation

$$y_1^n + 10 r_n y_1^{n-1} + \ldots + 10^n r_1 = 0 \ldots\ldots\ldots\ldots (1),$$

has one root, and one only, between 0 and 10; let this be ascertained by trial to be between b and $b+1$, so that it equals $b+z$ where z is between 0 and 1. Now let (1) be transformed into

$$(y_1-b)^n+\rho_n(y_1-b)^{n-1}+\ldots+\rho_1=0,$$
$$\text{or } z^n+\rho_n z^{n-1}+\ldots+\rho_1=0;$$

which has one root, and one only, between 0 and 1;

$$\therefore\ z_1^n+10\rho_n z_1^{n-1}+\ldots+10^n\rho_1=0,$$

has a root between 0 and 10, $=c+v$ suppose, where c is an integer found by trial, and v lies between 0 and 1. So that by carrying on this uniform process, we may obtain, to as many places of decimals as may be desired,

$$x=a+y=a+\frac{y_1}{10}=a+\frac{b}{10}+\frac{z}{10}=a+\frac{b}{10}+\frac{z_1}{100},$$

$$\text{or } x=a+\frac{b}{10}+\frac{c}{100}+\frac{d}{1000}+\&\text{c.}=a\,.\,bcd\ldots$$

b, c, d, &c. being written as the successive digits of the decimal part of the root.

If the root be greater than 10, we may, by a similar method, determine its successive digits.

Ex. 1. To find the positive root, lying between 1 and 2, of $x^3-3x-1=0$.

Writing down only the coefficients of the terms in the successive operations, we have

$$1 \quad 0 \quad -3 \quad -1 \text{ with a root} > 1 < 2.$$

Divide by $x-1$,

$$\begin{array}{llll} 1 & 1 & -2, & -3=r_1 \\ & 1 & 2, & 0=r_2 \\ & & 1, & 3=r_3 \end{array}$$

$$\therefore\ 1 \quad 3 \quad 0 \quad -3 \text{ has a root} > 0 < 1;$$

$$\therefore\ 1 \quad 30 \quad 0 \quad -3000 \left\{\begin{array}{l}\text{has a root} > 0 < 10\\ \text{or, by trial,} > 8 < \ 9\end{array}\right.$$

Divide by $x-8$,

$$\begin{array}{rrrl} 1 & 38 & 304, & -568 = r_1 \\ & 1 & 46, & 672 = r_2 \\ & & 1, & 54 = r_3 \end{array}$$

$$\therefore\ 1 \quad 54 \quad 672 \quad -568 \text{ has a root} > 0 < 1$$

$$\therefore\ 1 \quad 540 \quad 67200 \quad -568000 \left\{\begin{array}{l}\text{has a root} > 0 < 10\\ \text{or, by trial,} > 7 < \ 8\end{array}\right.$$

Divide by $x-7$,

$$\begin{array}{rrrl} 1 & 547 & 71029, & -70797 = r_1 \\ & 1 & 554, & 74907 = r_2 \\ & & 1, & 561 = r_3 \end{array}$$

$$\therefore\ 1 \quad 561 \quad 74907 \quad -70797 \text{ has a root} > 0 < 1$$

$$\therefore\ 1 \quad 5610 \quad 7490700 \quad -70797000 \left\{\begin{array}{l}\text{has a root} > 0 < 10\\ \text{or, by trial,} > 9 < 10\end{array}\right.$$

Divide by $x-9$, and repeat the same process, then the next decimal in the root will be determined, and so on for any number of decimals;

$$\therefore\ x = 1.879 \ldots$$

Ex. 2. To calculate the positive root, lying between 5 and 6, of

$$x^3 + 2x^2 - 23x - 70 = 0.$$

Diminishing the roots by 5 we find

$$(x-5)^3 + 17(x-5)^2 + 72(x-5) - 10 = 0,$$

having a value of $x-5$ between 0 and 1;

$$\therefore\ y^3 + 170y^2 + 7200y - 10000 = 0 \ \ldots\ldots\ldots \ (1),$$

has a root between 0 and 10, which by trial is found to be between 1 and 2.

Diminishing the roots of (1) by 1, we find

$$(y-1)^3 + 171(y-1)^2 + 7371(y-1) - 2629 = 0,$$

having a value of $y-1$ between 0 and 1;

$$\therefore\ z^3 + 1710z^2 + 737100z - 2629000 = 0 \ \ldots\ldots\ldots (2),$$

has a root between 0 and 10, which by trial is found to lie between 3 and 4.

Diminishing the roots of (2) by 3, we find

$$(z-3)^3 + 1713(z-3)^2 + 742239(z-3) - 402283 = 0$$

having a value of $z-3$ between 0 and 1;

$$\therefore\ v^3 + 17130v^2 + 74223900v - 402283000 = 0 \ \ldots\ldots (3),$$

has a root between 0 and 10, which by trial is found to lie between 4 and 5. Diminishing the roots of (3) by 4, we shall find the next decimal in the root to be 9; and so on; and we therefore have $x = 5.1349$.

CONTINUED FRACTIONS.

Before proceeding to the main object of finding the roots of equations under the forms of continued fractions, it will be necessary to investigate several general properties of that sort of expressions.

Every expression having the form

$$a + \cfrac{\beta}{b + \cfrac{\gamma}{c + \cfrac{\delta}{d + \ldots}}}$$

is called a continued fraction. We shall at present consider only the case where the numerators β, γ, δ, &c. are equal to unity, and the quantities a, b, c, &c., are positive integers; so that the continued fraction will be of the form

$$a + \cfrac{1}{b + \cfrac{1}{c + \cfrac{1}{d + \ldots}}} \qquad \text{or } a + \frac{1}{b+}\,\frac{1}{c+}\,\frac{1}{d+\ldots}$$

as it may be conveniently written.

Expressions of this sort present themselves, whenever we attempt to express numerically the values of fractional or irrational quantities.

For suppose we were required to estimate the value of a quantity, x, not expressible by an integer; if we first seek the whole number a which is next less than x, the difference $x-a$ is a fraction less than unity, which we may represent by $\frac{1}{y}$, y being a quantity greater than unity; similarly, if b be the whole number next less than y, the difference $y-b$ may be represented by $\frac{1}{z}$, z being a quantity greater than unity. Proceeding in this manner, we have

$$x=a+\frac{1}{y},\ \ y=b+\frac{1}{z},\ \ z=c+\frac{1}{u},\ \ u=d+\frac{1}{v},\ \&\text{c.},$$

$$\therefore\ x=a+\frac{1}{b+}\,\frac{1}{c+}\,\frac{1}{d+\ldots}.$$

If among the quantities x, y, z, &c., there occurs one which is exactly expressible by an integer, the continued fraction terminates; in the contrary case, it may be prolonged indefinitely. The former, as we proceed to shew, will happen whenever the quantity proposed to be transformed is a commensurable fraction; and the latter, when it is irrational or otherwise incommensurable; and the corresponding limited and unlimited continued fractions are called rational, and irrational, respectively.

128. To convert any proposed fraction $\frac{m}{n}$ into a continued fraction.

The integer next less than $\frac{m}{n}$ is the quotient of the division of m by n; let a be this quotient and p the remainder; then

$$\frac{m}{n}=a+\frac{p}{n}.$$

Similarly, let b be the quotient of the division of n by p, and q the remainder; then

$$\frac{n}{p}=b+\frac{q}{p}.$$

Again,

$$\frac{p}{q} = c + \frac{r}{q}, \text{ \&c.},$$

$$\therefore \frac{m}{n} = a + \frac{1}{b+} \frac{1}{c+\dots}.$$

Hence we see that, to reduce a vulgar fraction to a continued fraction, we must proceed exactly in the same manner as to find the greatest common measure of its numerator and denominator; taking care, however, first to divide the numerator by the denominator, so that when the numerator is less than the denominator, the first quotient, a, will be zero.

And as the process of finding the greatest common measure of two numbers always leads to a remainder zero, and a quotient expressed exactly by an integer, we see that every commensurable quantity can be expressed by a continued fraction which terminates; and conversely, every terminating continued fraction is the expression of a commensurable quantity; for by performing the calculations indicated, it can be reduced to an ordinary fraction.

Ex. By performing the process of finding the greatest common measure of 743 and 611, we find the quotients 1, 4, 1, 1, 1, 2, 3, 1, 3, and a remainder zero;

$$\therefore \frac{743}{611} = 1 + \frac{1}{4+} \frac{1}{1+} \frac{1}{1+} \frac{1}{1+} \frac{1}{2+} \frac{1}{3+} \frac{1}{1+} \frac{1}{3}.$$

Hence, also, it results that an incommensurable quantity can be converted only into a continued fraction which does not terminate; of which we shall now give an instance.

129. To convert $\sqrt{N}$ (N not being a complete square) into a continued fraction.

Let a^2 be the greatest square in N, so that $N = a^2 + b$; then a is the greatest integer in $\sqrt{N}$; let $\frac{1}{x_1}$ be the remainder;

$$\therefore\ x = \sqrt{N} = a + \frac{1}{x'}$$

$$\therefore\ x' = \frac{1}{\sqrt{N} - a} = \frac{\sqrt{N} + a}{b} = \alpha + \frac{1}{x''},\ \text{suppose},$$

α being the greatest integer in x', and $\frac{1}{x''}$ the remainder.

Suppose that, in continuing this process, we arrive at

$$x^{(r)} = \frac{\sqrt{N} + m}{n} = \mu + \frac{1}{y},$$

μ being the greatest integer in $x^{(r)}$, and $\frac{1}{y}$ the remainder;

$$\therefore\ y = \frac{n}{\sqrt{N} - (n\mu - m)} = \frac{n\,(\sqrt{N} + n\mu - m)}{N - (n\mu - m)^2} = \frac{\sqrt{N} + m'}{n'},$$

$$\text{if } m' = n\mu - m,\quad n' = \frac{N - (n\mu - m)^2}{n} = \frac{N - m'^2}{n};\quad (1)$$

$$\therefore\ y = \frac{\sqrt{N} + m'}{n'} = \mu' + \frac{1}{z},$$

μ' being the greatest integer in y, and $\frac{1}{z}$ the remainder.

Similarly, $z = \frac{\sqrt{N} + m''}{n''} = \mu'' + \frac{1}{u}$; &c.

m'', n'', being formed from m', n', μ', by precisely the same laws as m', n', were from m, n, μ, in equations (1); and μ'' being the nearest integer to z; and so on for the rest.

Hence y, z, &c. and the quotients μ', μ'', &c. will be found by an easy and uniform process, which must be continued till we arrive at a quotient $= 2a$; after which, the quotients will recur (as will be hereafter shewn) in the same order, beginning with a.

OBS. Since $m' = n\mu - m$, and $nn' = N - (n\mu - m)^2$, or $n' = n^0 + 2\mu m - n\mu^2$, since $nn^0 = N - m^2$;

($\frac{\sqrt{N} + m^0}{n^0}$ being the quantity which precedes $\frac{\sqrt{N} + m}{n}$);

we see that m and n will always be integers, since they are so in the first two cases, $\dfrac{\sqrt{N}+0}{1}$ and $\dfrac{\sqrt{N}+a}{b}$; and it will appear they are always positive.

Ex. 1. To express $\sqrt{23}$ by a continued fraction.

$\dfrac{\sqrt{23}+0}{1}=4$, writing down only the integral part;

also $m=0$, $n=1$, $\therefore m'=4.1-0=4$, $n'=\dfrac{23-16}{1}=7$,

$$\frac{\sqrt{23}+4}{7}=1 \qquad m''=7.1-4=3,\ n''=\frac{23-9}{7}=2,$$

$$\frac{\sqrt{23}+3}{2}=3 \qquad m'''=2.3-3=3,\ n'''=\frac{23-9}{2}=7,$$

$$\frac{\sqrt{23}+3}{7}=1 \qquad m^{iv}=7.1-3=4,\ n^{iv}=\frac{23-16}{7}=1,$$

$$\frac{\sqrt{23}+4}{1}=8 \qquad m^{v}=1.8-4=4,\ n^{v}=\frac{23-16}{1}=7,$$

$$\frac{\sqrt{23}+4}{7}=1.$$

Hence the quotients 1, 3, 1, 8 will recur; and consequently

$$\sqrt{23}=4+\frac{1}{1+}\ \frac{1}{3+}\ \frac{1}{1+}\ \frac{1}{8+}\ \frac{1}{1+}\ \frac{1}{3+\ldots},$$

Ex. 2. $\sqrt{7}=2+\dfrac{1}{1+}\ \dfrac{1}{1+}\ \dfrac{1}{1+}\ \dfrac{1}{4+}\ \dfrac{1}{1+\ldots}$.

CONVERGING FRACTIONS.

130. Returning to the consideration of the expression

$$x=a+\frac{1}{b+}\ \frac{1}{c+}\ \frac{1}{d+\ldots},$$

the fractions formed by taking 1, 2, 3, &c., of the quantities a, b, c, &c., are called converging fractions; thus

$$\frac{a}{1},\ a+\frac{1}{b}=\frac{ab+1}{b},\ a+\cfrac{1}{b+\cfrac{1}{c}}=\frac{abc+a+c}{bc+1},\ \&c.,$$

are converging fractions.

The converging fractions, taken in order, are alternately less and greater than the true value of x; thus $\frac{a}{1}$ is too small; $a+\frac{1}{b}$ is too large, because a part of the denominator is omitted; again, $b+\frac{1}{c}$ is too large, and therefore

$$a+\cfrac{1}{b+\cfrac{1}{c}}\ \text{is too small, and so on.}$$

The quantities a, b, c, &c., are called quotients; and any one with the quantity which must be added to it (supposing it were the last) to make the value of x exact, is called a complete quotient. Thus, using the notation of p. 155,

$$a+\frac{1}{y},\ b+\frac{1}{z},\ c+\frac{1}{u},\ \&c.,$$

are complete quotients.

131. To transform any continued fraction into a series of converging fractions.

Suppose $\frac{p}{q}$, $\frac{p'}{q'}$, $\frac{p''}{q''}$, three successive converging fractions.

Write down the quotients, and under them the converging fractions,

$$\begin{array}{cccccccc} a & b & c & d & \ldots & m & m' & m'' \\ \frac{a}{1} & \frac{ab+1}{b} & \frac{abc+a+c}{bc+1} & & \ldots & \frac{p}{q} & \frac{p'}{q'} & \frac{p''}{q''}. \end{array}$$

Now as far as we have gone we observe that, having formed the first two converging fractions, and written them one row in advance of the quotients, the numerator of any fraction is formed by multiplying the numerator of the preceding by the quotient that stands over it, and adding the numerator of the fraction preceding that; thus

$$abc + a + c = (ab + 1)\,c + a;$$

and the denominator, in the same manner, by multiplying the denominator of the preceding by the quotient over it, and adding the denominator preceding that;

$$\text{thus } bc + 1 = bc + \text{the denominator of } \frac{a}{1}.$$

Suppose the law to hold up to the quotient m, so that

$$\left(\frac{p^0}{q^0} \text{ being the fraction preceding } \frac{p}{q}\right)$$

$$p' = pm + p^0,\quad q' = qm + q^0;$$

$$\text{then } \frac{p'}{q'} = \frac{pm + p^0}{qm + q^0}.$$

Now $\frac{p''}{q''}$ differs from $\frac{p'}{q'}$ only in taking in another quotient, so that if $m + \frac{1}{m'}$ be written for m, we have

$$\frac{p''}{q''} = \frac{p\left(m + \frac{1}{m'}\right) + p^0}{q\left(m + \frac{1}{m'}\right) + q^0} = \frac{(pm + p^0)\,m' + p}{(qm + q^0)\,m' + q} = \frac{p'm' + p}{q'm' + q},$$

which is the same form as the preceding; if therefore the law hold for the formation of any one converging fraction, it holds for the formation of the next; but we have seen that it holds for the third, therefore the law obtains generally.

Ex. 1. To find a series of fractions converging to $\frac{743}{611}$.

Here the quotients are (Art. 128) 1, 4, 1, 1, 1, 2, 3, 1, 3; and the first two fractions are $\frac{1}{1}$, and $1 + \frac{1}{4}$ or $\frac{5}{4}$.

Hence, writing down the quotients and the first two fractions in the manner directed above, and forming the rest by the rule, we get

$$\begin{array}{ccccccccc} 1 & 4 & 1 & 1 & 1 & 2 & 3 & 1 & 3 \\ \frac{1}{1} & \frac{5}{4} & \frac{6}{5} & \frac{11}{9} & \frac{17}{14} & \frac{45}{37} & \frac{152}{125} & \frac{197}{162} & \frac{743}{611}; \end{array}$$

the last being the original fraction, and the preceding alternately greater and less than the true value.

If the proposed quantity has no integral part, then the first quotient, as was before observed, will be zero, and the first converging fraction $\frac{0}{1}$.

Ex. 2. To find a series of fractions converging to $\sqrt{23}$.

The quotients are (Art. 129) 4, 1, 3, 1, 8, 1, 3, 1, 8, ...

Hence we have

$$\begin{array}{ccccccccc} 4 & 1 & 3 & 1 & 8 & 1 & 3 & 1 & 8\ldots \\ \frac{4}{1} & \frac{5}{1} & \frac{19}{4} & \frac{24}{5} & \frac{211}{44} & \frac{235}{49} & \frac{916}{191} & \frac{1151}{240} & \ldots \end{array}$$

Ex. 3. Two scales, whose zero points coincide, are placed side by side, and the space between consecutive divisions in one is to that in the other as 1 to 1·06577; to find those divisions which most nearly coincide. They are 15 and 16, 61 and 65, 76 and 81, &c.

132. The difference between any two consecutive converging fractions, is a fraction whose numerator is unity, and denominator the product of the denominators of the fractions.

This is immediately verified with respect to the first two converging fractions; for

$$\frac{ab+1}{b} - \frac{a}{1} = \frac{1}{b}.$$

To prove, therefore, that it is generally true, it will be sufficient to consider three consecutive fractions $\frac{p^0}{q^0}$, $\frac{p}{q}$, $\frac{p'}{q'}$, and to shew that if the property holds for the two $\frac{p^0}{q^0}$, $\frac{p}{q}$, it must hold also for $\frac{p}{q}$ and $\frac{p'}{q'}$.

$$\text{Now } \frac{p'}{q'}-\frac{p}{q}=\frac{mp+p^0}{mq+q^0}-\frac{p}{q}=\frac{qp^0-pq^0}{(mq+q^0)q},$$

and by the hypothesis

$$\frac{p}{q}-\frac{p^0}{q^0}=\pm\frac{1}{qq^0}, \text{ or } pq^0-qp^0=\pm 1;$$

$$\therefore \frac{p'}{q'}-\frac{p}{q}=\frac{1}{q'q}, \text{ or } p'q\sim q'p=1.$$

133. In a series of converging fractions, each fraction approaches nearer to the value of the quantity to which the approximation is made, than that which precedes it; and (the integral part, or zero, being the first converging fraction) all the converging fractions of an odd order are less, and all those of an even order greater, than the true value.

$$\text{We have } \frac{p'}{q'}=\frac{mp+p^0}{mq+q^0};$$

and to deduce the value of x, the quantity to which the approximation is made, from that of $\frac{p'}{q'}$, it is sufficient to replace the quotient m by the complete quotient $m+\frac{1}{\mu}=y$ suppose, where y is always positive and greater than unity;

$$\therefore x=\frac{py+p^0}{qy+q^0};$$

$$\therefore x-\frac{p}{q}=\pm\frac{1}{q(qy+q^0)}, \quad \frac{p^0}{q^0}-x=\pm\frac{y}{q^0(qy+q^0)}.$$

Now $q^0<q$, and $y>1$, therefore on both accounts the value of $x-\frac{p}{q}$ is less than the value of $\frac{p^0}{q^0}-x$ (not regarding

the signs); therefore the successive converging fractions approach nearer and nearer to x.

Also since $\frac{p^0}{q^0} - x$ and $x - \frac{p}{q}$

have the same sign, the successive converging fractions are alternately greater and less than the true value; but the first converging fraction $\frac{a}{1}$ is less than x; therefore all the converging fractions of an odd order are less than x, and form an increasing series; and all the converging fractions of an even order are greater than x, and form a decreasing series.

134. All converging fractions are in their lowest terms.

For if the numerator and denominator of the fraction $\frac{p}{q}$ had a common measure, then from the equation $p'q - q'p = \pm 1$, it would follow that this common measure must divide unity.

135. The error, in taking any converging fraction for the value of the continued fraction, is less than unity divided by the product of the denominators of that fraction and the following one; and greater than unity divided by the product of that denominator and the sum of that denominator and the following one.

For, since $x - \frac{p}{q} = \pm \frac{1}{q(qy+q^0)}$,

and y is greater than m and less than $m+1$; therefore, leaving the sign out of consideration,

$$x - \frac{p}{q} < \frac{1}{q(qm+q^0)} > \frac{1}{q(qm+q+q^0)};$$

or, since $q' = qm + q^0$,

$$x - \frac{p}{q} < \frac{1}{qq'} > \frac{1}{q(q'+q)}.$$

136. We can also obtain a superior limit of the error, depending only on the denominator of that converging fraction

which we take for the approximate value; and an inferior limit, depending only on the denominator of the following one. For since q' is always greater than q,

$$\frac{1}{qq'} \text{ is less than } \frac{1}{q^2} \text{ and } \frac{1}{q(q'+q)} \text{ greater than } \frac{1}{2q'^2};$$

therefore, *a fortiori*,

$$x - \frac{p}{q} < \frac{1}{q^2} > \frac{1}{2q'^2}.$$

These limits are to be preferred, on account of their simplicity, to the former; and in most cases are sufficiently exact.

Hence we may at any step measure the accuracy of our approximation. Thus, in the examples of Art. 131, the fraction $\frac{152}{125}$, which converges towards $\frac{743}{611}$, differs from it by a quantity less than $\frac{1}{(125)^2}$ and greater than $\frac{1}{2(162)^2}$; and the fraction $\frac{916}{191}$, which converges towards $\sqrt{23}$, differs from it by a quantity less than $\frac{1}{(191)^2}$, and greater than $\frac{1}{2(240)^2}$.

Ex. To find a series of fractions converging to the value of the ratio of the circumference of a circle to its diameter; and to estimate the error with which each converging fraction is affected.

The value of this ratio, exact to ten places of decimals, is 3·1415926535; therefore, adding unity to the last decimal, the value of π will be comprised between the fractions

$$\frac{31\ 415\ 926\ 535}{10\ 000\ 000\ 000} \text{ and } \frac{31\ 415\ 926\ 536}{10\ 000\ 000\ 000}.$$

If now we perform the successive divisions for each fraction, we find the two series of quotients

3, 7, 15, 1, 292, 1, 1, 6

3, 7, 15, 1, 292, 1, 1, 1;

therefore, reserving only the quotients which are common to both, and which must belong to the continued fraction which expresses the value of π, and forming the converging fractions, we get

$$3,\ 7,\ 15,\ 1,\ 292,\ 1,\ 1,$$

$$\frac{3}{1},\ \frac{22}{7},\ \frac{333}{106},\ \frac{355}{113},\ \frac{103993}{33102},\ \frac{104348}{33215}.$$

These fractions are alternately greater and less than the true value of π; thus $\frac{22}{7}$ is too great; it is the ratio discovered by *Archimedes*, and differs from the true value by a quantity lying between

$$\frac{1}{7\times 106} \text{ and } \frac{1}{7\,(7+106)} \text{ or } \frac{1}{742} \text{ and } \frac{1}{791}.$$

The fraction $\frac{355}{113}$ is the value discovered by *Adrian Metius;* it is also too great, but far nearer than that of *Archimedes*, since it only leaves an error comprised between

$$\frac{1}{3740526} \text{ and } \frac{1}{3753295}.$$

137. In order that the fraction $\frac{p}{q}$ may differ from the exact value of x by a quantity less than a given quantity $\frac{1}{a}$, it is sufficient that we have $\frac{1}{q^2} < \frac{1}{a}$, or $q = \text{or} > \sqrt{a}$.

Hence we can always obtain, either exactly, or within any degree of approximation, the value of a quantity expressed by a continued fraction; for if the continued fraction terminates, we then obtain its value exactly; and if it does not terminate, we can obtain a converging fraction whose denominator satisfies the condition $q =$ or $> \sqrt{a}$, because the denominators of the converging fractions are integers, and go on increasing indefinitely.

138. In a series of converging fractions, each fraction differs less from the value of the quantity to which the approximation is made, than any other fraction in more simple terms.

Let $\frac{p}{q}$ be one of the converging fractions, and let $\frac{r}{s}$ be another fraction whose denominator is less than q. If $\frac{r}{s}$ be one of the converging fractions, the proposition is manifest from what has been proved. But if $\frac{r}{s}$ be not one of the converging fractions, then it cannot lie between $\frac{p}{q}$ and the preceding $\frac{p^0}{q^0}$; for if it could, then $\pm\left(\frac{p^0}{q^0} - \frac{r}{s}\right)$ would be less than $\frac{1}{q^0 q}$, or $\pm(p^0 s - q^0 r) < \frac{s}{q}$, which is impossible, because the first member of this inequality is an integer different from zero, and the second a proper fraction, since $s < q$.

Since then $\frac{r}{s}$ cannot lie between $\frac{p^0}{q^0}$ and $\frac{p}{q}$, if it lie to the right of $\frac{p}{q}$ (supposing the three arranged in order of magnitude) it differs from x more than $\frac{p}{q}$ does; and if it lie to the left of $\frac{p^0}{q^0}$, it differs from x more than $\frac{p^0}{q^0}$ does, and therefore *a fortiori* more than $\frac{p}{q}$ does.

139. Every periodic continued fraction is the expression for one of the roots of a quadratic equation whose coefficients are commensurable.

Let the continued fraction be

$$x = a + \frac{1}{b+\ldots}\,\frac{1}{k+}\,\frac{1}{l+}\,\frac{1}{y},$$

$$\text{where } y = r + \frac{1}{s+\ldots}\,\frac{1}{u+}\,\frac{1}{v+}\,\frac{1}{y};$$

so that $a, b, c, \ldots l$ are quotients which do not recur, and $r, s, \ldots v$ are those which recur indefinitely.

Let $\frac{p}{q}$, $\frac{p'}{q'}$, be converging fractions in the value of x, the last quotients comprised in them being, respectively, k and l; so that l and r are the quotients which stand over them, when formed according to the method of Art. 131; and let $\frac{P}{Q}$, $\frac{P'}{Q'}$, be converging fractions in the value of y, the last quotients comprised in them being, respectively, u and v; then, as in Art. 133,

$$x = \frac{p'y + p}{q'y + q}, \quad y = \frac{P'y + P}{Q'y + Q};$$

between which equations, eliminating y, we obtain an equation of the second degree in x, which demonstrates the property announced. When we wish to find x under an irrational form, we must take the positive value of y in the equation

$$Q'y^2 + (Q - P')\,y - P = 0,$$

and substitute it in the preceding value of x.

Ex.

$$x = a + \frac{1}{2a +}\,\frac{1}{2a +}\ldots; \quad \therefore\; x = a + \frac{1}{x + a}, \text{ or } x^2 = 1 + a^2.$$

LAGRANGE'S METHOD OF APPROXIMATION BY CONTINUED FRACTIONS.

140. To approximate to the roots of an equation by the method of continued fractions.

Let the equation $f(x) = 0$ have only one root between the integers a and $a + 1$; then writing $a + \frac{1}{y}$ for x, the first transformed equation will be

$$f(a) + f'(a)\,\frac{1}{y} + f''(a)\,\frac{1}{1.2y^2} + \ldots + \frac{1}{y^n} = 0 \;(1),$$

and since only one value of $\frac{1}{y}$ lies between 0 and 1, y has only one value greater than 1; if therefore we substitute successively 2, 3, 4, &c. for y, stopping at the first which gives a positive result, the integer preceding that, is the integral part of the value of y. Let this be b, and in (1) write $b+\frac{1}{z}$ for y; then the second transformed equation will have only one root greater than unity, the integral part of which, as before, will be the whole number next less than the one in the series 2, 3, 4, &c., which first gives a positive result when written for z; let this be c, and in the second transformed equation write $c+\frac{1}{u}$ for z, then the third transformed equation will have only one root greater than unity, the integral part of which may be found as before, and so on. We thus obtain successively the terms of a continued fraction

$$a+\frac{1}{b+}\,\frac{1}{c+}\,\frac{1}{d+\ldots},$$

which expresses the required value of x; consequently we are able (Art. 137) to find this value to any required degree of exactness.

If any of the numbers b, c, d, &c. is an exact root of the corresponding transformed equation, the process terminates, and we find the exact value of x. Also, if one of the transformed equations be identical with a preceding one, the continued fraction expressing the root is periodical; for, after that, the same quotients will recur in the same order; in this case a finite value, in the form of a surd, may be obtained for the root (Art. 139) by solving a quadratic whose coefficients are rational, both of whose roots will be roots of the proposed, (Art. 16) since the coefficients of the latter are supposed rational; consequently the first member of this quadratic will be a factor of the first member of the proposed equation, which may therefore be depressed two dimensions.

Ex. 1. To find the positive root of $x^3-2x-5=0$ under the form of a continued fraction.

Comparing this with $x^3-qx+r=0$, we find that

$$\frac{r^2}{4}-\frac{q^3}{27}=\frac{25}{4}-\frac{8}{27} \text{ is a positive quantity,}$$

therefore (p. 61) the equation has two impossible roots; and since its last term is negative, its third root is positive. Substituting 2 and 3, the results are -1 and $+16$, therefore the root lies between 2 and 3. Assume $x=2+\frac{1}{y}$, and the transformed equation is

$$y^3-10y^2-6y-1=0,$$

in which 10 and 11 being substituted give -61, $+54$. Assume $y=10+\frac{1}{z}$, and we obtain

$$61z^3-94z^2-20z-1=0,$$

whose root lies between 1 and 2. Proceeding in this manner we find

$$x=2+\frac{1}{10+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{2+\ldots}$$

the value of the root, in a continued fraction, which may be converted into a series of converging fractions.

Ex. 2. $x^3-7x+7=0$.

The roots which lie respectively between $1\frac{2}{3}$ and 2; $1\frac{1}{3}$ and $1\frac{2}{3}$; and -3, $-3\frac{1}{3}$; (Art. 49) will be found to be

$$1+\frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{4+}\,\frac{1}{y}; \quad 1+\frac{1}{2+}\,\frac{1}{1+}\,\frac{1}{4+}\,\frac{1}{y};$$

$$\text{and } -\left(3+\frac{1}{y}\right);$$

where y is the root greater than unity of

$$y^3-20y^2-9y+1=0;$$

In this case, therefore, the three roots terminate by the same quotient; a property that has been shewn to belong to the equation

$$(a'x)^3 - (1 + a + a^2)(3a'x - 2a - 1) = 0,$$

where a is any integer, and a' a divisor of $1 + a + a^2$. The example before us results from making $a = 4$, $a' = 3$.

141. When an equation has several roots between two consecutive integers, this method of approximating to them may be rendered easier by combining it with *Sturm's* theorem.

Substituting 0, 1, 2, 3, &c., successively for x in the series of quantities (Art. 101)

$$f(x),\ f_1(x),\ f_2(x),\ \ldots f_n(x) \ldots\ldots\ldots\ldots (1),$$

and noting between what substitutions, changes of sign are lost, and how many, we shall perceive between what integers the roots lie, and how many in each interval. For those roots which are situated singly between consecutive integers, the process will be that described above; but for those which lie in groups between consecutive integers, we must proceed as follows. Suppose several roots to lie between a and $a + 1$; substitute $a + \frac{1}{y}$ for x in series (1), and let the result be

$$\phi(y),\ \phi_1(y),\ \phi_2(y), \ldots \phi_n(y) \ldots\ldots\ldots\ldots (2);$$

then as many roots as $f(x) = 0$ has between a and $a + 1$, so many positive roots greater than unity will $\phi(y) = 0$ have; and if we write 1, 2, 3, &c., for y in series (2), and observe between what substitutions changes are introduced, the consecutive integers between which those values of y, either singly or in groups, are situated, will be determined. If there still be a group of values of y between consecutive integers b and $b + 1$, put $y = b + \frac{1}{z}$ in series (2), and let the result be

$$\psi(z),\ \psi_1(z),\ \psi_2(z), \ldots \psi_n(z) \ldots\ldots\ldots\ldots (3);$$

then as many roots as $\phi(y)=0$ has between b and $b+1$, so many positive roots greater than unity will $\psi(z)=0$ have; and, as before, substituting 1, 2, 3, &c., for z in series (3), and observing where the changes are introduced, we may determine the situation of those values of z; and the process must be continued till we arrive at a transformed equation whose positive roots are situated singly between consecutive integers; the approximation to each of these roots, as well as to all those already partially found, may then be continued, as in Art. 140, to any degree of accuracy. Thus all the values of x between a and $a+1$ will be determined; and the other groups of values of x, if there be any, must be treated in the same manner.

142. It is manifest that *Fourier's* method of separating the roots might be employed with similar advantages. For, being applied to the proposed equation $f(x)=0$, it would enable us to ascertain between what integers the roots lie, and how many in each interval. Next, being applied to the transformed equation

$$f\left(a+\frac{1}{y}\right)=0, \text{ or } \phi(y)=0,$$

(a and $a+1$ being one of those intervals,) it would point out between what integers the values of y lie, and how many in each interval. Similarly, in the next transformed equation

$$\phi\left(b+\frac{1}{z}\right)=0, \text{ or } \psi(z)=0,$$

b and $b+1$ being an interval containing more values of y than one, it would shew the situation of the values of z; and so on for all the transformed equations which it might be necessary to obtain, to completely separate the processes for approximating to each root of $f(x)=0$.

The following is an instance of the employment of *Sturm's* theorem.

Ex. $$f(x) = 6x^3 - 141x + 263,$$
$$f_1(x) = 6x^2 - 47,$$
$$f_2(x) = 94x - 263,$$
$$f_3(x) = +$$

	f	f_1	f_2	f_3
(2)	+	−	−	+
(3)	+	+	+	+;

hence two values of x lie between 2 and 3;

$$\therefore\ x = 2 + \frac{1}{y},$$

$$\phi(y) = 29y^3 - 69y^2 + 36y + 6,$$
$$\phi_1(y) = -23y^2 + 24y + 6,$$
$$\phi_2(y) = -75y + 94,$$
$$\phi_3(y) = +$$

	ϕ	ϕ_1	ϕ_2	ϕ_3
(1)	+	+	+	+
(2)	+	−	−	+

Hence two values of y lie between 1 and 2; and, putting $y = 1 + \frac{1}{z}$, it will be found that z has one value between 3 and 4, and another between 5 and 6; and the roots must now be approximated to by separate processes.

SOLUTION OF INDETERMINATE EQUATIONS OF THE FIRST ORDER BY CONTINUED FRACTIONS.

143. Another useful application of continued fractions is to find the integral values of x and y, which satisfy the indeterminate equation of the first order, $ax + by = c$.

We suppose a, b, c, to be integers positive or negative, and the two former prime to one another; for if they are not,

c must necessarily have the same divisor, since x and y represent integers. Let $x = \alpha$, $y = \beta$, be a solution, then

$$a\alpha + b\beta = c;$$

and therefore by subtraction,

$$a(x - \alpha) = -b(y - \beta);$$

but since a and b are prime to one another, $y - \beta$ must be a multiple of $a = at$ suppose; therefore $x - \alpha = -bt$,

$$\text{that is, } x = \alpha - bt, \; y = \beta + at,$$

where t is any integer positive or negative. Now to find α and β, resolve $\frac{a}{b}$ into a continued fraction; and in the series of converging fractions, let $\frac{p}{q}$ be that which immediately precedes $\frac{a}{b}$, then $pb - qa = \pm 1$, according as

$$\frac{p}{q} > \text{or} < \frac{a}{b};$$

$$\therefore cp \, . \, b - cq \, . \, a = \pm c;$$

hence, comparing this with the proposed equation, if the second members have the same sign, $\beta = cp$, $\alpha = -cq$; if different signs, $\beta = -cp$, $\alpha = cq$.

Ex. 1. $\qquad 5x + 7y = 29.$

$\frac{7}{5} = 1 + \frac{1}{2+} \frac{1}{2}$, and the converging fractions are $\frac{1}{1}, \frac{3}{2}, \frac{7}{5}$;

$$\therefore 3 \, . \, 5 - 7 \, . \, 2 = 1, \text{ and } 5 \, . \, 87 - 7 \, . \, 58 = 29;$$

$$\therefore x = 87 - 7t, \; y = -58 + 5t.$$

Ex. 2. $\qquad 11x + 13y = 190.$

$$x = 1140 - 13t, \; y = -950 + 11t.$$

144. When we wish to solve $ax + by = c$ in positive integers, t must be restricted in the general values

$$x = \alpha - bt, \; y = \beta + at.$$

First, suppose a and b to be positive, and therefore c positive since x and y are to be positive; then we must have

$\alpha - bt > 0$, $\beta + at > 0$, or $t < \frac{\alpha}{b}$ and $> -\frac{\beta}{a}$; therefore only those integral values of t which are comprised between the limits $-\frac{\beta}{a}$, $\frac{\alpha}{b}$ are admissible. These limits are never contradictory; for since α and β are positive or negative integers which satisfy the relation $a\alpha + b\beta = c$, we have $a\alpha + b\beta > 0$, and therefore $\frac{\alpha}{b} > -\frac{\beta}{a}$; but they may not include any integer, in which case the proposed equation has no solution in integers; and in no case has it more than a certain number of such solutions.

Secondly, let the equation be $ax - by = c$, a and b being positive; then $x = \alpha + bt$, $y = \beta + at$; and in order that these values may be positive, we must have $t > -\frac{\alpha}{b}$ and $t > -\frac{\beta}{a}$; hence we may give t any value above the greatest of these limits, so that the proposed equation will admit of an infinite number of solutions in positive integers.

In Ex. 1 (Art. 143) $t < 12\frac{3}{7} > 11\frac{3}{8}$; $\therefore$ t has only one value 12; and $x = 3$, $y = 2$ are the only positive integral values. Similarly, in Ex. 2, t has only one value 87.

The equation $ax + by + cz = d$ may be solved in positive integers, by assigning values 1, 2, 3, &c. to the variable whose coefficient is greatest, and of which consequently the admissible values lie within the narrowest limits; and solving, as above, the resulting equations.

Ex. 1. $10x + 9y + 7z = 58$. Here x can only have the values 1, 2 or 3. If $x = 1$, we get $9y + 7z = 48$, which admits of the single solution $y = z = 3$. If $x = 2$ or 3, we get the equations $9y + 7z = 38$, $9y + 7z = 28$, neither of which admits of a solution. Therefore the only solution of the proposed is $x = 1$, $y = z = 3$.

Ex. 2. $30x + 8y + 5z = 100$ is satisfied by the four systems of values for x, y, z respectively:

$$1, 5, 11;\ 1, 10, 8;\ 2, 5, 5;\ 2, 10, 2.$$

The equation $(mx + q)\,y = nx^2 + px + r$ may be solved in positive integers, by putting it under the form

$$m^2y = mnx - nq + mp + \frac{m^2r - mpq + nq^2}{mx + q},$$

and equating $mx + q$ successively to all the divisors of

$$m^2r - mpq + nq^2;$$

then if any one gives an integral value for x, that value can be substituted for x; and if the second member be then divisible by m^2, we shall obtain an integral value of y.

Thus $xy + x^2 = 2x + 3y + 29$ has two solutions,

$$x = 4,\ y = 21;\ \text{and}\ x = 5,\ y = 7.$$

PROPERTIES OF THE CONTINUED FRACTION WHICH EXPRESSES $\sqrt{N}$.

145. The last application we shall make of continued fractions shall be to determine the nature of the development of the square root of a number not a complete square, in that form; preparatory to which the following property must be demonstrated.

Let $\frac{1}{a+}\,\frac{1}{b+}\,\frac{1}{c+\ldots}\,\frac{1}{m+}\,\frac{1}{m'+}\,\frac{1}{m''}$ be the development of a proper fraction $\frac{P}{Q}$; then writing down the quotients and corresponding converging fractions, we have

$$a,\quad b,\quad c,\quad \ldots\ m,\ m',\ m'',$$

$$\frac{1}{a}\ \frac{b}{ab+1}\ \ldots\ \frac{p}{q}\ \frac{p'}{q'}\ \frac{p''}{q''}\ \frac{P}{Q},$$

whence we obtain the following equations:

$$Q = m''q'' + q', \quad \therefore \frac{q''}{Q} = \frac{1}{m'' + \frac{q'}{q''}};$$

$$q'' = m'q' + q, \quad \therefore \frac{q'}{q''} = \frac{1}{m' + \frac{q}{q'}};$$

$$q' = mq + q^0, \quad \therefore \frac{q}{q'} = \frac{1}{m + \frac{q^0}{q}}, \text{ \&c.};$$

$$\therefore \frac{q''}{Q} = \frac{1}{m''+}\;\frac{1}{m'+}\;\frac{1}{m+\ldots}\;\frac{1}{b+}\;\frac{1}{a};$$

that is, the development of $\frac{q''}{Q}$ in a continued fraction $\left(\frac{p''}{q''}\right.$ being the last of the series of fractions which converge to $\left.\frac{P}{Q}\right)$ gives the same quotients as the development of $\frac{P}{Q}$, but in an inverted order; if therefore in any case $q'' = P$, the series of quotients will be symmetrical, i.e. the same taken from the beginning and end, or of the form $a, b, c, \ldots c, b, a$.

146. If N be a whole number (not a complete square), then $\sqrt{N}$ may be developed in an indefinite continued fraction whose quotients recur in periods, the last quotient in each period being double of the greatest number whose square is less than N, and the period, as to the other quotients, being the same taken from the beginning and end.

In the continued fraction which expresses $\sqrt{N}$ (formed as explained in Art. 129), let the series of complete quotients, partial quotients, and converging fractions, be

$$\sqrt{N},\ \frac{\sqrt{N}+a}{b},\ldots\frac{\sqrt{N}+m^0}{n^0};\ \frac{\sqrt{N}+m}{n},\ \frac{\sqrt{N}+m'}{n'},\ldots\frac{\sqrt{N}+m_1^0}{n_1^0};\ \frac{\sqrt{N}+m}{n},\ldots$$

$$a,\quad \alpha,\ldots\quad \mu^0;\quad \mu,\quad \mu',\ldots\quad \omega;\quad \mu,\ldots$$

$$\frac{a}{1},\ldots\quad \frac{p^0}{q^0};\quad \frac{p}{q},\quad \frac{p'}{q'},\ldots\quad \frac{p_1^0}{q_1^0},\quad \frac{p_1}{q_1},\ldots$$

then any complete quotient $\frac{\sqrt{N}+m}{n}$ is formed from that which precedes it by the law $m' = \mu^0 n^0 - m^0$, $n' =$; and we must first shew that all the quantities m, n, m', n', &c., are positive integers. Suppose this to be the case up to m^0, n^0, then all the partial quotients up to μ^0 are positive integers, and the converging fractions up to $\frac{p}{q}$ inclusive can be formed in the usual way; and therefore, since $\frac{\sqrt{N}+m}{n}$ is the complete quotient corresponding to $\frac{p}{q}$, we have

$$\sqrt{N} = \frac{p\left(\frac{\sqrt{N}+m}{n}\right)+p^0}{q\left(\frac{\sqrt{N}+m}{n}\right)+q^0},$$

which, by equating rational and irrational parts, gives

$$\begin{aligned} pm + p^0 n &= qN, \\ qm + q^0 n &= p, \end{aligned} \quad \text{or} \quad \begin{cases} (pq^0 - qp^0)\, m = qq^0 N - pp^0, \\ (pq^0 - qp^0)\, n = p^2 - Nq^2. \end{cases}$$

But $pq^0 - qp^0 = +1$ or -1, according as $\frac{p}{q} >$ or $< \sqrt{N}$, therefore n is a positive integer; also the equation

$$qm + q^0 n = p \text{ gives } \frac{q^0}{q} = \frac{1}{n}\left(\frac{p}{q} - m\right);$$

and since $q > q^0$, $n > \frac{p}{q} - m$, and consequently $n > \sqrt{N} - m$;

$$\text{but } \frac{\sqrt{N}+m}{n} > \mu, \quad \therefore\ n < \sqrt{N} + m,$$

which would be impossible if m were negative. Hence m and n will be always positive integers, since they are so in the first two cases.

We can now find the limits which m and n cannot surpass, however far the process be carried on; for the equation $N - m^2 = nn^0$ shews that $m < \sqrt{N}$, and therefore m cannot exceed a the nearest integer to $\sqrt{N}$; and since $m + m^0 = \mu^0 n^0$, $2a$ is the limit both of n^0 and μ^0. But since the continued fraction which expresses $\sqrt{N}$ is unlimited, and since there can only be a certain number of values of m and n, the same value of m must occur with the same value of n an infinite number of times, that is, the same complete quotient must recur; and whenever this happens, then the succeeding quotients will be the same as those before obtained, and will recur in the same order; therefore the continued fraction which expresses $\sqrt{N}$ will (at least after a certain number of terms) be composed of a constant period of quotients, and we must now determine the point at which that period begins.

Suppose the recurring period of quotients to be

$$\mu,\ \mu',\ \mu'',\ \ldots\ldots\ \omega;$$

then since $N - m^2 = nn^0$, and $N - m^2 = nn_1^0$, $\therefore n^0 = n_1^0$;

$$\text{also since } m = \mu^0 n^0 - m^0,\quad m = \omega n_1^0 - m_1^0,$$

$$\therefore m^0 - m_1^0 = n^0(\mu' - \omega).$$

But the equation

$$qm + q^0 n = p \text{ gives } m = \frac{p}{q} - \frac{q^0}{q} n = a + \frac{r}{q} - \frac{q^0}{q} n,$$

since $\frac{p}{q}$, being an approximate value of $\sqrt{N}$, can only differ from a by a small fraction $\frac{r}{q}$;

$$\therefore a - m = n\frac{q^0}{q} - \frac{r}{q};$$

$$\text{therefore, since } q^0 < q,\quad a - m < n,$$

$$\text{hence } a - m^0 < n^0 \text{ and } a - m_1^0 < n^0;$$

$$\text{therefore } m^0 - m_1^0 < n^0 \text{ or } \frac{m^0 - m_1^0}{n^0} < 1,$$

but it also equals the integer $\mu^0 - \omega$; this integer then must equal zero, or $\omega = \mu^0$ and $m^0 = m_1^0$. In the same manner we can shew that the quotient which precedes ω is equal to that which precedes μ^0, and so on to the quotient α, so that α is the quotient which first recurs and with which therefore the period commences.

Hence the quotients and converging fractions may now be represented by

$$a;\ \alpha,\ \beta,\ \ldots\ \lambda,\quad \mu;\ \alpha,\ \beta,\ \ldots\ \lambda,\quad \mu;\ \alpha,\ \beta,\ \ldots$$
$$\frac{a}{1}\quad \ldots\frac{p^0}{q^0},\ \frac{p}{q};\ \frac{p'}{q'},\quad \ldots\frac{p_1^0}{q_1^0},\ \frac{p_1}{q_1};\ \frac{p_1'}{q_1'},\quad \ldots$$

Let z be the complete quotient of which μ, the last partial quotient in the first period, is the integral part, then

$$z - \mu = \sqrt{N} - a;$$

$$\therefore\ \sqrt{N} = \frac{pz + p^0}{qz + q^0} = \frac{p\sqrt{N} + p(\mu - a) + p^0}{q\sqrt{N} + q(\mu - a) + q^0};$$

$$\therefore\ p(\mu - a) + p^0 = Nq,\quad q(\mu - a) + q^0 = p;$$

$$\therefore\ \mu - a + \frac{q^0}{q} = \frac{p}{q},$$

or $\mu - a$ is the greatest integer in $\frac{p}{q}$ and therefore $= a$;

$$\therefore\ \mu = 2a.$$

Lastly, since

$$q^0 = p - aq,\ \text{ and } \frac{p^0 - aq^0}{q^0},\ \frac{p - aq}{q},$$

are consecutive converging fractions, and the development of the latter equals $\frac{1}{\alpha +}\ \frac{1}{\beta + \ldots}\ \frac{1}{\lambda}$, therefore (Art. 145) the period of quotients $\alpha, \beta, \gamma \ldots \kappa, \lambda$ is the same taken from the beginning and end, i. e. $\lambda = \alpha$, $\kappa = \beta$, &c. Hence the quotients proceed according to the law,

$$a;\ \alpha,\ \beta,\ \gamma,\ \ldots\ \gamma,\ \beta,\ \alpha,\ 2a;\ \alpha,\ \beta,\ \ldots\ \beta,\ \alpha,\ 2a;\ \alpha,\ \&c.$$

which law would be yet more regular, if the first quotient were either $2a$, or zero; i.e. if the irrational quantity developed were $\sqrt{N} \pm a$ instead of $\sqrt{N}$.

SOLUTION OF THE INDETERMINATE EQUATION OF THE SECOND ORDER, $x^2 - Ny^2 = \pm 1$.

147. Every converging fraction, $\frac{p}{q}$, which corresponds to the quotient $2a$ in any period, is such that $p^2 - Nq^2 = \pm 1$. For since $\mu = 2a$, the equation $m + m' = \mu n$, in which neither m nor m' can exceed a, will necessarily give $m = m' = a$, and $n = 1$; therefore the equation $(pq^0 - qp^0)\, n = p^2 - Nq^2$ becomes $p^2 - Nq^2 = \pm 1$ according as $\frac{p}{q} >$ or $< \sqrt{N}$.

Hence the equation $x^2 - Ny^2 = \pm 1$ may be always solved in whole numbers (at least with the upper sign) whatever be the number N (provided it be not a perfect square), in an infinite number of ways. If the number of terms in the period $a, \beta, \ldots \beta, a, 2a$, be even, all the fractions in the different periods corresponding to $2a$ will be $> \sqrt{N}$, and we shall obtain solutions only of $x^2 - Ny^2 = +1$; but if the period consist of an odd number of terms, then the first fraction which corresponds to $2a$ will be $< \sqrt{N}$, the second fraction corresponding to $2a > \sqrt{N}$, and so on; so that all fractions corresponding to $2a$ which stand in odd places will satisfy $x^2 - Ny^2 = -1$, and those in even places the equation

$$x^2 - Ny^2 = +1.$$

Ex. 1. $$x^2 - 23y^2 = 1.$$

For $\sqrt{23}$ we have (p. 161) the quotients and converging fractions,

$$4,\ 1,\ 3,\ 1,\ 8,\ 1,\ 3,\ 1,\ 8,\ \ldots$$

$$\frac{4}{1},\ \frac{5}{1},\ \frac{19}{4},\ \frac{24}{5}, \ldots\ldots\ldots\ldots\ldots \frac{1151}{240}, \ldots$$

$\therefore\ x = 24,\ y = 5$; or $x = 1151,\ y = 240$, &c.

Ex. 2. $$x^2 - 13y^2 = \pm 1;$$
With the upper sign $x = 18$, $y = 5$;
with the lower $x = 649$, $y = 180$.

The preceding investigation of the properties of the continued fraction which expresses $\sqrt{N}$, is taken from Legendre's *Essai sur la Théorie des Nombres.*

It may be observed that if p be a prime number, the polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$ or X possesses the remarkable property that the indeterminate equation

$$Y^2 - (-1)^{\frac{p-1}{2}} pZ^2 = 4X$$

can be satisfied by taking for Y and Z integral functions of x, in an infinite number of ways if $p = 4i + 1$, and in only one way if $p = 4i + 3$. If $p = 3$, the equation

$$4(x^2 + x + 1) = Y^2 + 3Z^2$$

admits the three solutions

$$Y = 2x + 1,\ Z = 1;\quad Y = x + 2,\ Z = x;\quad Y = x - 1,\ Z = x + 1.$$

SECTION VIII.

ON THE SYMMETRICAL FUNCTIONS OF THE ROOTS OF AN EQUATION.

---

148. A SYMMETRICAL function of the roots of an equation, as was before observed, is an expression in which each root is alike involved; and which is consequently made up of all the roots in such a manner that if any two be interchanged, its value is not altered. Thus

$$-p_1 = a + b + c + \dots + l, \quad p_2 = ab + ac + bc + \&c.,$$

and, in general, all the coefficients are symmetrical functions of the roots; for in these expressions, if b were written in every place where a occurs instead of a, and a in every place where b occurs instead of b, or if any other two of the roots were interchanged, the values of the expressions would not be altered. Our researches will be confined to those symmetrical functions which are rational.

149. We shall first consider the elementary cases where, in each term, only one, two, three, &c., of the roots are involved; viz.

$$a^m + b^m + c^m + d^m + \&c.,$$

$$a^m b^p + a^m c^p + b^m c^p + \&c.,$$

$$a^m b^p c^q + a^m c^p b^q + b^m a^p c^q + \&c.,$$

....

The first is formed by taking the sum of the roots each raised to the same power m, and consists o n terms.

The second is formed by taking all the permutations of the roots taken two together, and affecting the first letter

in each product with the index m, and the second with the index p; and it consists of $n(n-1)$ terms.

The third is formed by taking all the permutations of the roots taken three together, and affecting the first letter in each product with the index m, the second with the index p, and the third with the index q; and it consists of

$$n(n-1)(n-2) \text{ terms.}$$

Similarly, the symmetrical function each term of which contained r roots, would be formed by taking all the permutations of the roots taken r together, and in each product affecting the first letter with the index m, the second with the index p, the third with the index q, and so on; and it would consist of $n(n-1)(n-2) \dots (n-r+1)$ terms. (The above supposes all the indices m, p, q, &c., to be **unequal**: we shall afterwards revert to the case where some of them are equal.)

Since, therefore, in the above cases, any term being given, all the others may be deduced from it, by forming all the permutations of the letters which compose it, and affecting the letters in each with the indices taken always in the same order; we may denote them by the symbol Σ prefixed to any one of the terms, thus

$$\Sigma(a^m), \quad \Sigma(a^m b^p), \quad \Sigma(a^m b^p c^q);$$

and the first, that is, the sum of the m^{th} powers of the roots may be indifferently expressed by $\Sigma(a^m)$ or S_m; we shall generally employ the latter, as the sums of similar powers of the roots are the simplest sort of symmetrical functions, and are the quantities by which all others are expressed.

150. The value of every *rational* symmetrical function of the roots of an equation can be expressed by the coefficients, without knowing the actual values of the roots, as we shall shew. But it will be necessary to consider only the case of integral functions; because when the terms of a symmetrical function are fractional, we can, by reducing them to a common

denominator, express the function by a single fraction whose numerator and denominator are integral symmetrical functions.

Thus $\frac{ab}{2c^2}+\frac{ac}{2b^2}+\frac{bc}{2a^2}-3abc$, which is a fractional symmetrical function of the three quantities, a, b, c, becomes by reduction $\frac{a^3b^3+a^3c^3+b^3c^3-6a^3b^3c^3}{2a^2b^2c^2}$.

In the elementary cases of Art. 149, the indices are the same, and of course have their sum the same, in every term of each; i.e. the function is homogeneous; if a symmetrical function should present itself not fulfilling these two conditions, it can be separated into two or more symmetrical functions that do fulfil them; so that the only symmetrical functions necessary to be considered are those which, besides being rational and integral, are homogeneous, and such that each has the same indices in every one of its terms.

NEWTON'S THEOREM FOR THE SUMS OF THE POWERS OF THE ROOTS

151. To express the sum of the m^{th} powers of the roots of an equation in terms of the coefficients, and the sums of the inferior powers.

We have (Art. 60)

$$f'(x)=\frac{f(x)}{x-a}+\frac{f(x)}{x-b}+\ldots+\frac{f(x)}{x-l};$$

therefore, effecting the divisions, which can all be exactly performed, since a, b, ... l are roots of $f(x)=0$, we get (Art. 6)

$$\frac{f(x)}{x-a}=x^{n-1}+(a+p_1)x^{n-2}+(a^2+p_1a+p_2)x^{n-3}+\ldots$$
$$+(a^m+p_1a^{m-1}+p_2a^{m-2}+\ldots+p_m)x^{n-m-1}+\&c.$$

$$\frac{f(x)}{x-b} = x^{n-1} + (b+p_1)\,x^{n-2} + (b^2+p_1b+p_2)\,x^{n-3} + \dots$$
$$+ (b^m + p_1b^{m-1} + p_2b^{m-2} + \dots + p_m)\,x^{n-m-1} + \&c.$$
$$\dots\dots = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\frac{f(x)}{x-l} = x^{n-1} + (l+p_1)\,x^{n-2} + (l^2+p_1l+p_2)\,x^{n-3} + \dots$$
$$+ (l^m + p_1l^{m-1} + p_2l^{m-2} + \dots + p_m)\,x^{n-m-1} + \&c.$$

Hence, adding these quotients together, we have

$$f'(x) = nx^{n-1} + (S_1 + np_1)\,x^{n-2} + (S_2 + p_1S_1 + np_2)\,x^{n-3} + \dots$$
$$+ (S_m + p_1S_{m-1} + p_2S_{m-2} + \dots + p_{m-1}S_1 + np_m)\,x^{n-m-1} + \&c.$$

But $f'(x) = nx^{n-1} + (n-1)\,p_1x^{n-2} + (n-2)\,p_2x^{n-3} + \dots$

$$\dots + (n-m)\,p_mx^{n-m-1} + \&c.;$$

hence, equating the coefficients of corresponding terms in these identical expressions, we get

$$S_1 + np_1 = (n-1)\,p_1, \quad \text{or } S_1 + p_1 = 0;$$
$$S_2 + p_1S_1 + np_2 = (n-2)\,p_2, \quad \text{or } S_2 + p_1S_1 + 2p_2 = 0; \ \&c.,$$
$$S_m + p_1S_{m-1} + p_2S_{m-2} + \dots p_{m-1}S_1 + np_m = (n-m)\,p_m,$$
$$\text{or } S_m + p_1S_{m-1} + p_2S_{m-2} + \dots + p_{m-1}S_1 + mp_m = 0,$$

the formula which gives the sum of the m^{th} powers (m being less than n) of the roots, in terms of the coefficients and the sums of the inferior powers; and by means of which the sums of all similar powers whose index is less than the degree of the equation, can be successively expressed by integral functions of the coefficients.

But if m be equal to or greater than n, multiplying the equation by x^{m-n}, we have

$$x^m + p_1x^{m-1} + p_2x^{m-2} + \dots + p_nx^{m-n} = 0;$$

therefore, replacing x successively by all the roots $a, b, c, \dots l$, and taking the sum of the results, we have

$$S_m + p_1S_{m-1} + p_2S_{m-2} + \dots + p_nS_{m-n} = 0. \quad (1)$$

Hence, making $m = n,\ n+1,\ n+2$, &c., successively, we find, observing that

$$S_0 = a^0 + b^0 + c^0 + \ldots + l^0 = n,$$

$$S_n + p_1 S_{n-1} + p_2 S_{n-2} + \ldots + n p_n = 0,$$

$$S_{n+1} + p_1 S_n + p_2 S_{n-1} + \ldots + p_n S_1 = 0, \text{ \&c.}$$

Hence the sums of all similar powers whatever of the roots, can be expressed by integral functions of the coefficients.

OBS. The sums of the powers of the roots of any equation S_1, S_2, S_3, &c., form what is called a Recurring Series; that is, a series in which an equation of the first degree with constant coefficients holds good between a certain definite number of consecutive terms, in whatever part of the series they be taken; for, any one of them, S_n, depends, when the equation is complete, upon the n preceding, by the equation (1), in which the constants of relation are the coefficients of the equation.

152. To find the sums of the negative similar powers of the roots, we must write $\frac{1}{y}$ for x, and apply the above formulæ to the transformed equation in y.

153. We may observe that by the preceding method the value of $\phi(a) + \phi(b) + \ldots + \phi(l)$, (where $\phi(x)$ denotes any rational algebraic function) may be readily found. For,

$$\frac{f'(x) \cdot \phi(x)}{f(x)} = \frac{\phi(x)}{x-a} + \frac{\phi(x)}{x-b} + \ldots + \frac{\phi(x)}{x-l};$$

therefore, performing the divisions, and reserving only the remainders, (Art. 6)

$$\frac{Ax^{n-1} + Bx^{n-2} + \text{\&c.}}{f(x)} = \frac{\phi(a)}{x-a} + \frac{\phi(b)}{x-b} + \ldots + \frac{\phi(l)}{x-l};$$

$$\therefore Ax^{n-1} + Bx^{n-2} + \text{\&c.} = x^{n-1}\{\phi(a) + \phi(b) + \ldots + \phi(l)\} + \text{\&c.};$$

$\therefore \phi(a) + \phi(b) + \ldots + \phi(l) = A =$ coefficient of the highest power of x, in the remainder of the division of $f'(x) \,.\, \phi(x)$ by $f(x)$.

154. In practical applications to equations of a low degree, or consisting of a small number of terms, we may, instead of calculating the sums of the powers successively from one another, express them immediately in terms of the coefficients of the equation, by the following method.

For x write $\dfrac{1}{y}$ in the identical equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + p_3 x^{n-3} + \ldots + p_n = (x-a)(x-b) \times (x-c) \ldots (x-l);$$

$$\therefore 1 + p_1 y + p_2 y^2 + p_3 y^3 + \ldots + p_n y^n = (1-ay)(1-by) \times (1-cy) \ldots (1-ly).$$

Hence, taking the *Napierian* logarithms of both sides,

$$p_1 y + \left.\begin{matrix} p_2 \\ -\frac{1}{2}p_1^2 \end{matrix}\right\} y^2 + \left.\begin{matrix} p_3 \\ -p_1p_2 \\ +\frac{1}{3}p_1^3 \end{matrix}\right\} y^3 + \left.\begin{matrix} p_4 \\ -p_1p_3 \\ -\frac{1}{2}p_2^2 \\ +p_1^2p_2 \\ -\frac{1}{4}p_1^4 \end{matrix}\right\} y^4 +$$

$$= -yS_1 - \tfrac{1}{2}y^2S_2 - \tfrac{1}{3}y^3S_3 - \tfrac{1}{4}y^4S_4 - \text{\&c.};$$

therefore, equating coefficients,

$$S_1 = -p_1,$$
$$S_2 = -2p_2 + p_1^2,$$
$$S_3 = -3p_3 + 3p_1p_2 - p_1^3,$$
$$S_4 = -4p_4 + 4p_1p_3 + 2p_2^2 - 4p_1^2p_2 + p_1^4, \text{ \&c.};$$

and, in general, $S_m =$ coefficient of y^m in the expansion, by ascending powers of y, of $-m \log \left\{ y^n f\left(\dfrac{1}{y}\right) \right\}$.

Ex. 1. $\qquad x^4 + rx + s = 0.$

Let $x^4 + rx + s = (x-a)(x-b)(x-c)(x-d)$;

$\therefore 1 + y^3(r + sy) = (1-ay)(1-by)(1-cy)(1-dy)$;

$$\therefore\ y^3(r+sy)-\tfrac{1}{2}y^6(r+sy)^2+\&c.=-yS_1-\tfrac{1}{2}y^2S_2-\tfrac{1}{3}y^3S_3$$
$$-\tfrac{1}{4}y^4S_4-\tfrac{1}{5}y^5S_5-\tfrac{1}{6}y^6S_6-\&c.;$$

hence, equating coefficients, we have

$$S_1=0,\ S_2=0,\ S_3=-3r,\ S_4=-4s,\ S_5=0,\ S_6=3r^2.$$

Ex. 2. The sum of the m^{th} powers of the roots of $x^n-1=0$ is n, when m is a multiple of n; and zero in all other cases.

Let $\qquad x^n-1=(x-a)(x-b)\ldots(x-l);$

$$\therefore\ 1-y^n=(1-ay)(1-by)\ldots(1-ly);$$

$$\therefore\ y^n+\tfrac{1}{2}y^{2n}+\ldots+\frac{1}{r}y^{rn}+\&c.=yS_1+\tfrac{1}{2}y^2S_2+\ldots+\frac{1}{rn}y^{rn}S_{rn}+\&c.;$$

$$\therefore\ S_1=S_2=\ldots=0,$$
$$S_n=S_{2n}=\ldots=S_{rn}=n.$$

Ex. 3. To express the sum of the m^{th} powers of the roots of a quadratic in terms of its coefficients.

Let $\qquad x^2-px+q=(x-a)(x-b);$

$$\therefore\ 1-y(p-qy)=(1-ay)(1-by);$$

therefore, taking the *Napierian* logarithms of both sides, and writing down only the terms which, when developed, will involve y^m, we have

$$\frac{y^m}{m}(p-qy)^m+\frac{y^{m-1}}{m-1}(p-qy)^{m-1}+\frac{y^{m-2}}{m-2}(p-qy)^{m-2}+\&c.$$
$$=\frac{1}{m}y^mS_m+\&c.;$$

therefore, equating coefficients of y^m,

$$S_m=p^m-mp^{m-2}q+\frac{m(m-3)}{1\,.\,2}p^{m-4}q^2-\ldots$$
$$+(-1)^r\frac{m(m-r-1)(m-r-2)\ldots(m-2r+1)}{1\,.\,2\,.\,3\ldots r}p^{m-2r}q^r+\&c.$$

Hence, if $q=1$, $b=\frac{1}{a}$, $p=a+\frac{1}{a}$; and the value of $a^m+\frac{1}{a^m}$ in terms of $a+\frac{1}{a}$, is given by the series

$$S_m = p^m - mp^{m-2} + \dots$$
$$+ (-1)^r . \frac{m(m-r-1)(m-r-2)\dots(m-2r+1)}{1.2.3\dots r} p^{m-2r} + \&c.$$

Ex. 4. $$x^n - px^{n-1} + q = 0.$$

S_m = coefficient of y^m in expansion of $-m \log\{1-y(p-qy^{n-1})\}$

$$= p^m - mp^{m-n}q + \frac{m(m-2n+1)}{1.2} p^{m-2n}q^2$$
$$- \frac{m(m-3n+2)(m-3n+1)}{1.2.3} p^{m-3n}q^3 + \&c.$$

155. Similarly, we may express the coefficients immediately in terms of the sums of the powers. For since (Art. 151)

$$\log_e(1+p_1y+p_2y^2+p_3y^3+\dots+p_ny^n) = -yS_1 - \tfrac{1}{2}y^2S_2$$
$$-\tfrac{1}{3}y^3S_3 - \&c.$$

$$\therefore\ 1+p_1y+p_2y^2+p_3y^3+\&c. = e^{-yS_1-\frac{1}{2}y^2S_2-\frac{1}{3}y^3S_3-\dots}$$
$$= 1 - yS_1 - \left.\begin{matrix}\tfrac{1}{2}S_2 \\ +\tfrac{1}{2}(S_1)^2\end{matrix}\right\} y^2 - \left.\begin{matrix}\tfrac{1}{3}S_3 \\ +\tfrac{1}{2}S_1S_2 \\ -\tfrac{1}{6}(S_1)^3\end{matrix}\right\} y^3 - \&c.$$

hence, equating coefficients,

$$p_1 = -S_1,$$
$$p_2 = -\tfrac{1}{2}S_2 + \frac{1}{1.2}(S_1)^2,$$
$$p_3 = -\tfrac{1}{3}S_3 + \frac{1}{1.2}S_1S_2 - \frac{1}{1.2.3}(S_1)^3,$$
$$\dots = \dots$$

Ex. $$x^6 + p_2x^4 + p_3x^3 + p_4x^2 + p_5x + p_6 = 0.$$

Here $S_1 = 0$, and proceeding as above, and in the development of the second member reserving only powers of y as far as the sixth, we have

$$1 + p_2 y^2 + p_3 y^3 + p_4 y^4 + p_5 y^5 + p_6 y^6 = e^{-\frac{1}{2}y^2 S_2 - \frac{1}{3}y^3 S_3 - \dots}$$

$$= 1 - \frac{y^2}{1}\left(\tfrac{1}{2}S_2 + \tfrac{1}{3}yS_3 + \tfrac{1}{4}y^2 S_4 + \tfrac{1}{5}y^3 S_5 + \tfrac{1}{6}y^4 S_6\right)$$

$$+ \frac{y^4}{1\,.\,2}\left(\tfrac{1}{2}S_2 + \tfrac{1}{3}yS_3 + \tfrac{1}{4}y^2 S_4\right)^2 - \frac{y^6}{1\,.\,2\,.\,3}\left(\tfrac{1}{2}S_2\right)^3;$$

$$\therefore\ p_2 = -\tfrac{1}{2}S_2,\quad p_3 = -\tfrac{1}{3}S_3,$$

$$p_4 = -\tfrac{1}{4}S_4 + \frac{1}{1\,.\,2}\left(\tfrac{1}{2}S_2\right)^2,$$

$$p_5 = -\tfrac{1}{5}S_5 + \frac{1}{1\,.\,2}\,\tfrac{1}{3}S_2 S_3.$$

$$p_6 = -\tfrac{1}{6}S_6 + \frac{1}{1\,.\,2}\left\{\tfrac{1}{4}S_2 S_4 + \frac{1}{9}(S_3)^2\right\} - \frac{1}{1\,.\,2\,.\,3}\left(\tfrac{1}{2}S_2\right)^3.$$

USE OF THE SUMS OF SIMILAR POWERS OF THE ROOTS IN APPROXIMATING TO THE VALUES, REAL OR IMAGINARY, OF THE ROOTS.

156. The employment of the sums of similar powers of the roots, was first pointed out by *Newton* as a method of approximating to the greatest root, in the following proposition.

If in the series S_1, S_2, S_3, &c., formed by the sums of the powers of the roots of an equation, each term be divided by that which precedes it, the successive quotients continually converge to the greatest root, provided it be real.

Suppose a, b, $\rho\,(\cos\theta \pm \sqrt{-1}\,\sin\theta)$, &c., to be the roots, arranged in order of numerical magnitude, each pair of imaginary roots being estimated in that respect by its modulus (Art. 85), then

$$\frac{S_{m+1}}{S_m} = \frac{a^{m+1} + b^{m+1} + 2\rho^{m+1}\cos(m+1)\theta + \&c.}{a^m + b^m + 2\rho^m \cos m\theta + \&c.}$$

$$= a \cdot \frac{1 + \left(\frac{b}{a}\right)^{m+1} + \left(\frac{\rho}{a}\right)^{m+1} 2\cos(m+1)\theta + \&c.}{1 + \left(\frac{b}{a}\right)^m + \left(\frac{\rho}{a}\right)^m 2\cos m\theta + \&c.}$$

supposing the greatest root to be real;

which {since the fractions $\left(\frac{b}{a}\right)^m$, $\left(\frac{b}{a}\right)^{m+1}$, &c., may, by the increase of m, be made as small as ever we please} approaches to a as its limit; and therefore $\frac{S_{m+1}}{S_m}$ is an approximation to the greatest root provided it be real, becoming closer and closer as m increases. But if there be a pair of imaginary roots whose modulus exceeds the greatest of the real roots, then

$$\frac{S_{m+1}}{S_m} = \rho \cdot \frac{2\cos(m+1)\theta + \left(\frac{a}{\rho}\right)^{m+1} + \left(\frac{b}{\rho}\right)^{m+1} + \&c.}{2\cos m\theta + \left(\frac{a}{\rho}\right)^m + \left(\frac{b}{\rho}\right)^m + \&c.}$$

and therefore, by the increase of m, approximates to

$$\rho \frac{\cos(m+1)\theta}{\cos m\theta},$$

which may evidently have any value.

157. Again, according as the two greatest roots are real or imaginary, we have

$$S_m = (a^m + b^m)\left(1 + \frac{2\rho^m \cos m\theta}{a^m + b^m} + \frac{c^m}{a^m + b^m} + \&c.\right),$$

$$\text{or } = \rho^m \left\{2\cos m\theta + \left(\frac{a}{\rho}\right)^m + \left(\frac{b}{\rho}\right)^m + \&c.\right\}.$$

Hence, whether a and b be real or imaginary, provided they be the two greatest roots, we shall have, by the continual increase of m,

$$S_m = a^m + b^m \text{ nearly},$$
$$S_{m+1} = a^{m+1} + b^{m+1},$$
$$S_{m+2} = a^{m+2} + b^{m+2},$$

each equation being nearer to the truth than the preceding;

$$\therefore\ S_m \cdot S_{m+2} - S^2_{m+1} = (ab)^m (a-b)^2, \quad (u_m)$$

$$S_{m+1} \cdot S_{m+3} - S^2_{m+2} = (ab)^{m+1} (a-b)^2, \quad (u_{m+1})$$

and the quotient of the latter divided by the former, $= ab$.

This shews that if from every three terms of the series S_1, S_2, S_3, &c., another series $\Sigma(u_m)$ be formed by subtracting the square of the mean from the product of the extremes, then the quotients obtained by dividing each term of the new series by that term which precedes it, continually converge to the product of the two greatest roots.

When the two greatest roots are real, since the first is already known, the second becomes known by the process just described. When they are imaginary, as their product is known, it remains to determine their sum, which may be done as follows. We have

$$S_m S_{m+3} - S_{m+1} S_{m+2} = a^m b^m (a+b)(a-b)^2, \quad (v_m)$$

and dividing this by u_m we get a result $= a + b$; which shews that if from every four terms of the series S_1, S_2, S_3, S_4, &c. another series $\Sigma(v_m)$ be formed by subtracting the product of the means from that of the extremes: then the quotients obtained by dividing each term of this series by the corresponding term of the series $\Sigma(u_m)$ continually converge to the sum of the two greatest roots.

Hence the product and sum of the two imaginary roots being known, each of them can be found. This is the chief method yet known for approximating, with tolerable facility, to the real and imaginary parts of impossible roots.

Ex. 1. $\qquad x^3 - 10x^2 - 6x - 1 = 0$

$\Sigma(S_m) = 10,\ 112,\ 1183,\ 12512,\ 132330,\ 1399555,\ 14202042$, &c.

$$\therefore\ a = \frac{14202042}{1399555} = 10{\cdot}576.$$

Ex. 2. $x^4 - x^3 + 4x^2 + x - 4 = 0.$

$\Sigma(S_m) = 1, -7, -14, 29, 96, -34, -503, -347, 2083, 3838, -6159,$

$\Sigma(u_m) = \quad -63, -399, -2185, -10202, -49444, -241211, -1168158,$

$\Sigma(v_m) = \quad -69, -266, -2308, -11323, -50414, -245363, -1207713;$

the first series being a divergent one, shews that a and b are imaginary;

$$\text{the second gives } ab = \frac{1168158}{241211} = 4.84,$$

$$\text{the second and third give } a + b = \frac{1207713}{1168158} = 1.03;$$

$$\therefore\ a = \frac{1}{2}(1.03 + 4.3\sqrt{-1}),\quad b = \frac{1}{2}(1.03 - 4.3\sqrt{-1}).$$

The remaining roots c and d may be found from the equations

$$c + d + 1.03 = 1,\quad cd = -\frac{4}{4.84}.$$

THEOREMS FOR EXPRESSING SYMMETRICAL FUNCTIONS OF THE ROOTS BY THE COEFFICIENTS.

158. Every rational symmetrical function of the roots of an equation can be expressed by the coefficients of that equation.

First, to find the value of the double function $\Sigma(a^m b^p)$.

If we multiply together the two equations

$$S_m = a^m + b^m + c^m + \dots + l^m,$$
$$S_p = a^p + b^p + c^p + \dots + l^p,$$

we have
$$S_m S_p = a^{m+p} + b^{m+p} + c^{m+p} + \dots + l^{m+p}$$
$$+ a^m b^p + a^m c^p + b^m a^p + \&c.$$

Now the first line is equal to S_{m+p}; and the second consists of all the permutations of the roots taken two together, the first letter in each being affected with the index m, and the second with the index p, and is therefore equal to the double function $\Sigma(a^m b^p)$;

$$\therefore\ S_m S_p = S_{m+p} + \Sigma(a^m b^p),$$
$$\text{or } \Sigma(a^m b^p) = S_m S_p - S_{m+p} \dots (1).$$

Next, to find the value of the triple function $\Sigma(a^m b^p c^q)$. Multiplying together the equations

$$\Sigma(a^m b^p) = a^m b^p + a^m c^p + b^m a^p + \&c.,$$
$$S_q = \quad a^q + \quad b^q + \quad c^q + \&c.,$$

the result will consist of three different partial products;

(1) the sum of products of the form $a^{m+q} b^p = \Sigma(a^{m+q} b^p)$,

(2) the sum of products of the form $a^m b^{p+q} = \Sigma(a^m b^{p+q})$,

(3) the sum of products of the form $a^m b^p c^q = \Sigma(a^m b^p c^q)$;

$$\therefore\ S_q \Sigma(a^m b^p) = \Sigma(a^{m+q} b^p) + \Sigma(a^m b^{p+q}) + \Sigma(a^m b^p c^q),$$

a formula which enables us to calculate a triple function from knowing how to calculate a double one.

Hence, replacing $\Sigma(a^m b^p)$, $\Sigma(a^{m+q} b^p)$, $\Sigma(a^m b^{p+q})$, by their values obtained from formula (1), we have

$$\Sigma(a^m b^p c^q) = S_m S_p S_q - S_{m+p} S_q - S_{m+q} S_p - S_{p+q} S_m + 2 S_{m+p+q}.$$

In the same manner might the quadruple function $\Sigma(a^m b^p c^q d^r)$, or the sum of any succeeding combinations, be expressed by the sums of the powers; and as these latter are expressible by integral functions of the coefficients, it follows that all the above symmetrical functions can be expressed by integral functions of the coefficients. And as every symmetrical polynomial in a, b, c, &c. must be composed of the assemblage, by addition or subtraction of several symmetrical functions of the form $\Sigma(a^m b^p c^q \ldots)$, it follows that the value of every rational symmetrical function whatever of the roots of an equation (without the roots being known) can be expressed by the coefficients of the equation.

Obs. The above expressions for the elementary symmetrical functions will require to be modified, when any of the indices become equal. Thus, if $m = p$ in the formula

$$\Sigma(a^m b^p) = S_m S_p - S_{m+p},$$

since $a^m b^p = b^m a^p$, the terms in $\Sigma(a^m b^p)$ will become equal two and two, and $\Sigma(a^m b^p)$ will be reduced to $2\Sigma(a^m b^m)$;

$$\therefore\ \Sigma(a^m b^m) = \tfrac{1}{2}(S_m^2 - S_{2m}).$$

Similarly, if $m=p=q$ in $\Sigma(a^m b^p c^q)$, the six combinations formed by interchanging a, b, c, in $a^p b^q c^r$ are reduced to one, and $\Sigma(a^m b^p c^q)$ is reduced to $6\Sigma(a^m b^m c^m)$;

$$\therefore \Sigma(a^m b^m c^m) = \tfrac{1}{6}S^3_m - \tfrac{1}{2}S_{2m}S_m + \tfrac{1}{3}S_{3m};$$

and in general, if t of the exponents become equal, the general formula must be divided by $1.2.3 \ldots t$. If $\Sigma(a^m b^p c^q \ldots)$ have r roots in each term, it will consist, as we have seen, of $n(n-1)\ldots(n-r+1)$ terms; and if t of the indices become equal, it will consist of $\dfrac{n(n-1)\ldots(n-r+1)}{1.2.3\ldots t}$ terms.

Ex. 1. Let the roots of $x^3+px^2+qx+r=0$ be a, b, c, to find the value of $\Sigma(a^2 b)$.

$$\begin{aligned}\Sigma(a^2 b) &= S_1 S_2 - S_3 \\ &= (-p)(p^2-2q) - (-3r+3pq-p^3) \quad \text{(Art. 151)} \\ &= 3r - pq.\end{aligned}$$

Ex. 2. Let the roots of $x^n - 1 = 0$ be a, b, c, &c., to find the value of $\Sigma(a^m b^p)$.

$$\Sigma(a^m b^p) = S_m S_p - S_{m+p}.$$

Hence the value is n^2-n, when m and p are both multiples of n; and $-n$, when $m+p$ only is a multiple of n; and zero, in all other cases. (Ex. 2, Art. 151.)

Ex. 3. Let the roots of $x^n + p_1 x^{n-1} + \ldots + p_n = 0$ be a, b, c, &c., to find the value of $\Sigma(a^2 b^2 c)$. It will be found to be

$$p_1 p_2 p_3 - 3p_1^2 p_4 - 3p_3^2 + 4p_2 p_4 + 7p_1 p_5 - 12p_6.$$

159. Any rational function whatever of a root of an equation of the n^{th} degree, can be reduced to an integral function at most of $n-1$ dimensions; or to a fraction whose numerator is at most of $m-1$ dimensions, and denominator of $n-m$ dimensions, if the proposed function be integral and of m dimensions.

If $a, b, c, \ldots l$ be the n roots of $f(x)=0$, and if the proposed function of one of them a be integral, and of the form

$$F(a) = A_0 + A_1 a + \ldots + A_m a^m,$$

where m is greater than n; then considering $f(x)$ as divisor, and forming the identical equation

$$F(x) = f(x) \times Q + R,$$

and making $x = a$, we get $F(a) = R$, where R is at the most of $n - 1$ dimensions in a.

We may therefore always suppose the dimension m of $F(a)$ to be less than n; and now taking $F(x)$ for divisor, and forming the identity

$$f(x) = F(x) \times Q' + R',$$

and making $x = a$, we get $F(a) = -\dfrac{R'}{Q'}$, where R' is at the most of $m - 1$ dimensions in a, and Q' of $n - m$ dimensions.

But if $F(a)$ the proposed function be fractional $= \dfrac{\phi(a)}{\psi(a)}$ suppose, then,

$$\frac{\phi(a)}{\psi(a)} = \phi(a) \cdot \frac{\psi(b)\,\psi(c)\ldots\psi(l)}{\psi(a)\cdot\psi(b)\ldots\psi(l)} \ldots\ldots\ldots\ldots (1);$$

the denominator is a symmetrical function of the roots of $f(x) = 0$, and can be expressed by the coefficients of $f(x) = 0$. The numerator is similarly an integral symmetrical function of the roots of $\dfrac{f(x)}{x - a} = 0$, and can be expressed in terms of the coefficients of that equation; that is, in terms of a and the coefficients of $f(x) = 0$; therefore the equation (1) takes the form

$$\frac{\phi(a)}{\psi(a)} = A_0 + A_1 a + \ldots + A_m a^m,$$

and is reduced to the preceding case.

By the same method any rational function of several roots of an equation, may be replaced by an integral function of the same roots. For if other roots $b, c, \ldots$ of $f(x) = 0$, be contained in the expression $\dfrac{\phi(a)}{\psi(a)}$, this latter may in the first place be put under the form

$$A_0 + A_1 a + \ldots + A_m a^m,$$

where A_0, A_1, &c. are rational functions of the coefficients of $f(x)=0$, and of b, c, &c.; then the quantities A_0, A_1, &c., can be rendered integral with respect to another root b; then with respect to another root c; and so on, till the expression is rendered integral with respect to all the roots involved in it.

TRANSFORMATION OF EQUATIONS BY SYMMETRICAL FUNCTIONS.

The theory of symmetrical functions will enable us to transform an equation, whose roots are unknown, into another whose roots are all the combinations, formed after an assigned law, of the roots of the proposed, taken two, three, &c. at a time. We shall first exemplify the method in the following transformation, as being the most convenient practical one of solving a problem of considerable interest.

160. To transform an equation into one whose roots are the squares of the differences of its roots.

Let $a, b, c, \ldots l$ be the n roots of the proposed, then the roots of the transformed equation will be

$$(a-b)^2, \ (a-c)^2, \ (b-c)^2, \text{ \&c.},$$

in number $\frac{1}{2}n(n-1)$, since they include all the combinations of the n quantities $a, b, c, \ldots l$ taken two together; hence the degree of the transformed equation will be $\frac{1}{2}n(n-1)=m$ suppose.

Let the transformed equation be

$$y^m + q_1 y^{m-1} + q_2 y^{m-2} + q_3 y^{m-3} + \ldots + q_m = 0,$$

and let $s_1, s_2, \ldots s_i$ denote the sums of the first, second, &c., i^{th} powers of its roots; then (Art. 155) all the coefficients may be expressed by these sums, thus

$$q_1 = -s_1, \ q_2 = -\tfrac{1}{2}(s_2 + q_1 s_1), \ q_3 = -\tfrac{1}{3}(q_2 s_1 + q_1 s_2 + s_3), \text{ \&c.};$$

therefore it only remains to calculate s_1, s_2, &c. Now if S_1, S_2, &c., denote, as usual, the sums of the powers of the roots of the proposed equation, and k be any positive integer, we have

$$(x-a)^k+(x-b)^k+\ldots+(x-l)^k = nx^k - kS_1x^{k-1}$$
$$+\frac{k(k-1)}{1.2}S_2x^{k-2}-\ldots+(-1)^kS_k.$$

Therefore, changing x successively into $a, b, c \ldots l$, and taking the sum of the resulting equations, we have

$$(a-b)^k+(a-c)^k+\ldots+(a-l)^k+(b-a)^k+(b-c)^k+\ldots$$
$$+(b-l)^k+\ldots$$
$$= nS_k - kS_1S_{k-1}+k\frac{(k-1)}{1.2}S_2S_{k-2}-\ldots+(-1)^knS_k.$$

Now if k be an odd number, each member of this equation is separately zero; but if k be an even number and $=2i$, then the value of the first member is $2s_i$; and in the second member, the terms are equal, taken from the beginning and end;

$$\therefore\ s_i = nS_{2i} - 2iS_1S_{2i-1}+\frac{2i(2i-1)}{1.2}S_2S_{2i-2}-\ldots$$
$$+\tfrac{1}{2}(-1)^i\frac{2i(2i-1)\ldots(i+1)}{1.2.3\ldots i}S_i^2.$$

Hence to form the equation whose roots are the squares of the differences of the roots of

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots+p_n=0,$$

or, as it is called, the equation of differences, we must first calculate S_1, S_2, S_3, &c., in terms of p_1, p_2, &c.; and next s_1, s_2, s_3, &c., by the formula just investigated; and lastly q_1, q_2, q_3, &c., the coefficients of the required equation, by the method of (Art. 155).

161. We have seen one use of the equation of differences (Art. 40), viz. to determine a limit less than the least difference

of the roots of a proposed equation; another is to determine, within certain limits, the number of impossible roots which the proposed equation contains.

If the transformed equation be complete and have no continuations of sign, it cannot have a negative root; and therefore the primitive equation has no impossible roots, because a pair must give rise to a real negative root in the equation of differences; but if the transformed equation have continuations of sign, then it has either impossible or negative roots; and as these can only arise from impossible roots in the proposed equation, it follows that this latter has impossible roots. Also if the proposed equation have p possible roots, and if the difference of no two of its imaginary roots be a real quantity, the transformed equation will have $\frac{p(p-1)}{2}$ positive roots, and the rest will be either negative or imaginary; hence if the last term of the transformed equation be positive, $\frac{p(p-1)}{2}$ is even; and therefore p, which must be of the same parity as n, will be of the form $4m$ or $4m+1$, according as n is even or odd. Similarly, if the last term of the transformed equation be negative, it may be shewn that the number of real roots in the proposed equation will be of the form $4m+2$ or $4m+3$, according as n is even or odd.

Ex. 1. $x^3 - 2x - 5 = 0$. The equation of differences is

$$y^3 - 12y^2 + 36y + 643 = 0,$$

which has not all its roots positive; therefore the proposed has impossible roots.

Ex. 2. To transform $x^4 + rx + s = 0$ into one whose roots shall be the squares of the differences of its roots.

Here, by Ex. (Art. 154), and by the formulæ of Arts. 160 and 155, we have

$$S_1 = 0, \quad S_2 = 0, \quad S_3 = -3r, \quad S_4 = -4s, \quad S_5 = 0,$$
$$S_6 = 3r^2, \quad S_7 = 7rs, \quad S_8 = 4s^2, \quad S_9 = -3r^3,$$
$$S_{10} = -10r^2s, \quad S_{11} = -11rs^2, \quad S_{12} = -4s^3 + 3r^4;$$
$$s_1 = 0, \quad s_2 = -16s, \quad s_3 = -78r^2, \quad s_4 = 576s^2,$$
$$s_5 = -10r^2s, \qquad s_6 = -7936s^3 + 2190r^4;$$
$$q_1 = 0, \quad q_2 = 8s, \qquad q_3 = 26r^2, \quad q_4 = -112s^2,$$
$$q_5 = 216r^2s, \qquad q_6 = 256s^3 - 27r^4.$$

Hence the transformed equation is

$$y^6 + 8sy^4 + 26r^2y^3 - 112s^2y^2 + 216r^2sy + 256s^3 - 27r^4 = 0.$$

Hence if the last term be positive, or $\left(\frac{s}{3}\right)^3 > \left(\frac{r}{4}\right)^4$, the number of real roots in the proposed will be of the form of $4m$; but there cannot be more than two, therefore there are none. If the last term be negative, or $\left(\frac{s}{3}\right)^3 < \left(\frac{r}{4}\right)^4$ the number of real roots of the proposed will be of the form $4m + 2$, and therefore there will be two. These results agree with those found at p. 62.

Obs. The absolute or final term of the equation of differences, which put equal to zero expresses the condition for the proposed having equal roots, and in most cases is the only one wanted, is a symmetrical function of the roots of the first derived equation; and we shall shew that it can be calculated for any equation, supposing its expression determinable for an equation of the next inferior degree.

Let q_m, q_{m-1} denote, respectively, the product of the squares of the differences of the roots of $f(x) = 0$, and of

$$\frac{f(x)}{x-a} = x^{n-1} + (a + p_1)^{n-2} + \&c. = 0 \ \ldots \ (1),$$

$$\therefore \ q_m = q_{m-1}(a-b)^2(a-c)^2 \ldots (a-l)^2 = q_{m-1} \times \{f'(a)\}^2.$$

But, by the supposition, q_{m-1} can be expressed in terms of the coefficients of (1), that is, of a and p_1, p_2, &c., and there-

fore q_m, being an integral function of one of the roots of $f(x)=0$, can be reduced (Art. 159) to the form

$$q_m = A_0 + A_1 a + A_2 a^2 + \ldots + A_{n-1} a^{n-1}.$$

But since q_m is a symmetrical function of the n roots $a, b, \ldots l$, this equation must still remain true when $b, c, \ldots l$, are severally substituted for a; hence it is satisfied by n quantities and is only of $n-1$ dimensions;

$$\therefore\ q_m = A_0.\quad \text{(Art. 14).}$$

Ex. $$x^3 + px^2 + qx + r = 0.$$

Here $\dfrac{f(x)}{x-a} = x^2 + (a+p)\,x + a^2 + pa + q$, hence (Art. 84)

$$q_2 = (b-c)^2 = (a+p)^2 - 4(a^2+pa+q) = -3a^2 - 2pa + p^2 - 4q;$$

$$\{f'(a)\}^2 = (3a^2 + 2pa + q)^2 = (p^2-3q)\,a^2 + (pq-9r)\,a + q^2 - 3pr,$$

reducing by the relation

$$a^3 = -pa^2 - qa - r.\quad (2)\quad \text{Hence}$$

$$-q_3 = (3a^2 + 2pa + 4q - p^2)\,\{(p^2-3q)\,a^2 + (pq-9r)\,a + q^2 - 3pr\}$$
$$= \{3(p^2-3q)\,a + 2p^3 - 3pq - 27r\}\,a^3 + \ldots + (4q-p^2)(q^2-3pr),$$

and as we only want the term independent of a when this is reduced so as to contain no power of a higher than the second by relation (2), we get by successive substitutions

$$q_3 = \{3(p^2-3q)\,a + 2p^3 - 3pq - 27r\}\,(pa^2+qa+r) + \ldots$$
$$+ (p^2-4q)(q^2-3pr)$$
$$= (p^2-4q)(q^2-3pr) + (2p^3-3pq-27r)\,r + 3p\,(p^2-3q)\,a^3 + \&c.$$
$$= (p^2q^2 - p^3r - 4q^3 + 9pqr - 27r^2 - 3pr\,(p^2-3q) + A_1 a + A_2 a^2.$$
$$\therefore\ q_3 = p^2q^2 - 4p^3r - 4q^3 + 18pqr - 27r^2.$$

In the particular case of a biquadratic equation, Mr Cayley has shewn that, if it be put under the form

$$ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0,$$

and if $I = ae - 4bd + 3c^2$, $J = ace + 2bcd - ad^2 - eb^2 - c^3$,

then $\alpha, \beta, \gamma, \delta$ being the four roots,

$$a^6(\alpha-\beta)^2(\alpha-\gamma)^2(\alpha-\delta)^2(\beta-\gamma)^2(\beta-\delta)^2(\gamma-\delta)^2 = 16\,(I^3 - 27J^2).$$

162. Besides the method of Art. 160, we may also transform an equation by means of symmetrical functions, as follows.

Suppose that each root of the transformed equation is to be a rational function, $\phi(a, b, c, \&c.)$, of any number of the roots of the proposed equation; then having formed all the combinations $\phi(a, b, c, \&c.)$, $\phi(a, c, d, \&c.)$, &c., the transformed equation, resolved into its factors, will be

$$\{y - \phi(a, b, c, \&c.)\}\{y - \phi(a, c, d, \&c.)\} \ldots = 0;$$

and as this product is not altered by interchanging a, b, c, &c., among themselves, (for the only effect of that is to place its factors in a different order) we are certain that, after multiplication, the coefficients of the different powers of y will be symmetrical functions of a, b, c, &c., and may therefore be expressed by the coefficients of the proposed equation.

Hence if we can discover a rational function of four letters which, when the letters are permuted in all possible ways, admits of only three values, we may transform a biquadratic into a cubic; and the roots of the cubic may be so composed of the roots of the biquadratic, as to lead to the determination of the latter. It is evident that each of the expressions $ab+cd$, and $(a+b-c-d)^2$, answers the abovenamed condition; and we proceed to apply to the solution of a biquadratic this method, which has for its leading feature the circumstance that we can form functions of four letters which admit of only three values.

Ex. 1. To transform $x^4 + px^3 + qx^2 + rx + s = 0$, roots a, b, c, d, into one whose roots shall be

$$ab + cd, \quad ac + bd, \quad ad + bc;$$

the transformed equation is

$$\{y - (ab + cd)\}.\{y - (ac + bd)\}.\{y - (ad + bc)\} = 0,$$

in which the coefficient of y^2 evidently $= -q$,

the coefficient of y

$$= \Sigma(a^2bd) = (a + b + c + d)(abc + abd + acd + bcd) - 4abcd$$

$$= pr - 4s,$$

and the last term with its sign changed

$$= \Sigma(a^3bcd) + \Sigma(a^2b^2c^2) = (p^2 - 2q)s +$$
$$r^2 - 2\Sigma(a^2b^2cd) = (p^2 - 2q)s + r^2 - 2qs;$$
$$\therefore y^3 - qy^2 + (pr - 4s)y - (r^2 - 4qs + p^2s) = 0, \ldots (1).$$

Ex. 2. Hence, also, we can transform the proposed equation into one whose roots shall be

$$(a+b-c-d)^2, \quad (a+c-b-d)^2, \quad (a+d-b-c)^2.$$

For let $z = (a+b-c-d)^2$

$$= (a+b+c+d)^2 - 4(ab+ac+ad+bc+bd+cd)$$
$$+ 4(ab+cd) = p^2 - 4q + 4y;$$
$$\therefore y = \frac{z - p^2 + 4q}{4};$$

and substituting in (1), the transformed equation in z is

$$z^3 - (3p^2 - 8q)z^2 + (3p^4 - 16p^2q + 16q^2 + 16pr - 64s)z$$
$$- (p^3 - 4pq + 8r)^2 = 0.$$

Either of these transformed equations may be employed in the solution of the proposed biquadratic. Thus, in the first case, let α be a value of y, then $ab + cd = \alpha$; $abcd = s$; therefore ab and cd are known; also

$$ab(c+d) + cd(a+b) = -r, \quad (a+b) + (c+d) = -p;$$

therefore $a+b$, and $c+d$ are known; hence all the roots are obtained from one root of the reducing cubic. In the second case, if we know $z_1\ z_2\ z_3$ the three values of z, by means of these, and the equation $a+b+c+d = -p$, we can find the roots of the biquadratic merely by addition and subtraction; or they may all be expressed by a single formula

$$4x = \sqrt{z_1} + \sqrt{z_2} + \sqrt{z_3} - p,$$

where the first two radicals carry double signs; and the sign of the third radical is determined by the relation

$$\sqrt{z_1}\,\sqrt{z_2}\,\sqrt{z_3} = -p^3 + 4pq - 8r.$$

Ex. 3. To transform $x^3+px^2+qx+r=0$, roots a, b, c, into

$$y^3+\frac{1}{4}p'y^2+\frac{1}{16}q'y+\frac{1}{64}r'=0,$$

whose roots are

$$\frac{(a+b)^2}{4ab},\ \frac{(a+c)^2}{4ac},\ \frac{(b+c)^2}{4bc}.$$

It will be found that $-p'=\frac{pq}{r}+3$, (Art. 21)

$$q'=\frac{\Sigma(a^3b^3)}{a^2b^2c^2}+\frac{\Sigma(a^3)+5\Sigma(a^2b)}{abc}+12$$

$$=\frac{q^3}{r^2}-\frac{(q-p^2)p}{r}+3$$

$$-r'=\left\{\frac{\Sigma(a^2b)}{abc}+2\right\}^2=\left\{\frac{pq}{r}-1\right\}^2.$$

163. To transform an equation into another which shall want an assigned number of terms.

Let the given equation be

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots+p_n=0\ldots\ldots\ldots\ldots(1),$$

and assume

$$y=a_0+a_1x+a_2x^2+\ldots+a_mx^m\ldots\ldots\ldots\ldots(2),$$

where a_0, a_1, &c. are indeterminate, and $m<n$. Since y has the same number of values as x, the transformed equation in y, resulting from the elimination of x between (1) and (2), will be of the n^{th} degree. This elimination may be performed by means of symmetrical functions, as follows. Raising equation (2) to the r^{th} power, and not admitting any power of x greater than x^n by means of (1), we get

$$y^r=A_0+A_1x+A_2x^2+\ldots+A_{n-1}x^{n-1},$$

where A_0, A_1, &c. are integral homogeneous functions of a_0, a_1, &c. of the r^{th} degree. Hence substituting for x its n values in this equation, and taking the sum of the results,

$$S_r=nA_0+A_1s_1+A_2s_2+\ldots+A_{n-1}s_{n-1}\ldots\ldots(3),$$

where s_r, S_r, denote, respectively, the sum of the r^{th} powers of the roots of the proposed equation, and of the transformed equation in y, which suppose to be

$$y^n + q_1 y^{n-1} + q_2 y^{n-2} + \ldots + q_n = 0 \ldots\ldots\ldots (4),$$

then (Art. 155)

$$q_1 = -S_1, \quad q_2 = -\tfrac{1}{2}S_2 + \tfrac{1}{2}S_1^2, \text{ \&c.};$$

so that by means of (3) all the coefficients q_1, q_2, &c. can be expressed in terms of a_0, a_1, &c. and the coefficients of (1). Now suppose that we wish to exterminate m successive terms beginning with the second in (4), then we must have

$$S_1 = 0, \quad S_2 = 0, \text{ \&c. } S_m = 0;$$

but as these equations are respectively of 1, 2, &c. m dimensions in a_0, a_1, ... a_m; therefore the determination of these quantities, one of which may be taken arbitrarily, will depend by Bezout's theorem on an equation of the degree $1.2.3\ldots m$. If we wish to exterminate all the terms except the first and last, the problem will depend on the solution of an equation of the degree $1.2.3\ldots(n-1)$.

Ex. 1. To solve $x^3 + px^2 + qx + r = 0$, by taking away its second and third term.

Assume $$y = a + bx + x^2 \ldots\ldots\ldots\ldots\ldots (1),$$

and let the transformed equation in y be

$$y^3 + Py^2 + Qy + R = 0;$$

then from the equations $P = 0$, $Q = 0$, which are respectively of the first and second degree in a and b, those two quantities may be determined, and expressed by the coefficients of the proposed. The equation in y is then reduced to $y^3 + R = 0$, and furnishes three values of y. But, squaring and cubing (1), and reducing by means of the proposed, we get

$$y^2 = b_0 + b_1 x + b_2 x^2,$$
$$y^3 = c_0 + c_1 x + c_2 x^2;$$

which two equations along with (1), will furnish a value of x expressed rationally by y, y^2, and y^3; so that the three values of x become known from those of y.

Ex. 2. To solve $x^4+px^3+qx^2+rx+s=0$ by taking away its second and fourth terms.

Assume $$y=a+bx+x^2,$$

and let the transformed equation in y be

$$y^4+Py^3+Qy^2+Ry+S=0;$$

then from the equations $P=0$, $R=0$, which are respectively of the first and third degrees in a and b, those two quantities may be determined and expressed by the coefficients of the proposed, by means of the solution of the Cubic.

The equation in y is thus reduced to

$$y^4+Qy^2+S=0,$$

which can be solved as a quadratic, and will furnish four values of y; then, as in the preceding example, obtaining the values of y^2, y^3, and y^4 under the forms

$$y^2=b_0+b_1x+b_2x^2+b_3x^3, \text{ \&c.},$$

we get a value of x expressed rationally by the first four powers of y; so that the four values of x become known from those of y.

This method of solving the general equations of the third and fourth degree is known as *Tschirnhausen's* Method.

Ex. 3. To take away the second, third, and fourth terms of $x^n+p_1x^{n-1}+\ldots+p_n=0$, by means of the solution of a single cubic equation.

Assume $$y=a_0+a_1x+a_2x^2+a_3x^3+a_4x^4,$$
and let the transformed equation in y be

$$y^n+q_1y^{n-1}+q_2y^{n-2}+\ldots+q_n=0.$$

Then by what was shewn above, S_r the sum of the r^{th} powers of the roots of this equation is a homogeneous function of the quantities a_0, $a_1 \ldots a_4$ of the r^{th} degree; consequently the coefficients q_1, q_2, &c. are homogeneous functions of those same quantities, the degree of each being equal to its subscribed

index. To make the second, third, and fourth terms of the transformed equation disappear, we must have

$$q_1 = 0, \quad q_2 = 0, \quad q_3 = 0;$$

the first of these is linear, let a_0 be determined from it in terms of a_1, a_2, a_3, a_4, and substituted in the other two, and suppose the latter to become $Q_2 = 0$, $Q_3 = 0$; Q_2, Q_3 being respectively homogeneous functions of the second and third orders, of the four quantities a_1, a_2, a_3, a_4. Hence Q_2 may be put under the form

$$P^2 a_4^2 + 2PQa_4 + R, \text{ or } (Pa_4 + Q)^2 + R - Q^2,$$

where P is a constant, and Q, R, homogeneous functions of a_1, a_2, a_3, respectively of the first and second degrees: similarly $R - Q^2$, being a homogeneous function of the second order of the three quantities a_1, a_2, a_3, can be resolved into a square, and a homogeneous function of two of them a_1, a_2; and this latter can be reduced to the form

$$(P'a_1 + Q'a_2)^2 + (R'a_1)^2,$$

so that by these reductions $Q_2 = 0$ assumes the form

$$f^2 + g^2 + h^2 + k^2 = 0,$$

where f, g, h, k are linear functions of a_1, a_2, a_3, a_4; and this equation may be satisfied by making

$$f^2 + g^2 = 0, \quad h^2 + k^2 = 0; \quad \text{or } f = g\sqrt{-1}, \quad h = k\sqrt{-1}.$$

These latter equations are linear and give a_3, a_4 in terms of a_1 and a_2; and if the values of a_3, a_4 be substituted in $Q_3 = 0$, its first member will become a homogeneous function of the 3rd order, of a_1 and a_2; and if either a_1 or a_2 be taken arbitrarily, the other will be determined by solving a cubic equation. Thus the values of a_0, a_3, a_4 become known, and the transformed equation in y is

$$y^n + q_4 y^{n-4} + \dots + q_n = 0.$$

By the same transformation the second, third, and fifth terms may be made to disappear from any equation, but the determination of $a_0, a_1 \dots a_4$ will require the solution of an equation of the fourth degree, instead of a cubic. Hence also

it appears that by this process, joined to the transformation which consists in replacing the unknown quantity by its inverse, we may exterminate in any equation either the second, third and fourth terms from the end; or the second, third and fifth terms from the end; and in equations of the fifth degree, we may exterminate any three terms between the first and last, the solution at most of a biquadratic equation being required. This application of *Tschirnhausen's* method is due to Mr Jerrard.

164. To determine the roots of $f(x)=0$, an equation of the n^{th} degree, having given one of the values of a rational function of them that is susceptible of $1.2.3\ldots n$ distinct values by the permutations of the roots.

Let V denote this rational function, and V_1 the given value of it; also by $V_1, V_2, \ldots V_r$ let the $r=1.2.3\ldots(n-1)$ values be denoted, which V assumes when in its expression the $n-1$ quantities $x_2, x_3, \ldots x_n$ are permuted in all possible ways without changing the place of x_1. We may hence form an equation in V of the r^{th} degree

$$(V-V_1)(V-V_2)\ldots(V-V_r)=0\ldots\ldots\ldots\ldots(1),$$

whose roots are all different, and whose coefficients, being symmetrical functions of $x_2, x_3, \ldots x_n$ the roots of

$$f(x)\div(x-x_1)=0,$$

can be expressed rationally by the coefficients of the proposed equation and x_1. Then the first member of (1) takes the form $F(V, x_1)$; and as (1) is satisfied by $V=V_1$, we have indentically $F(V_1, x_1)=0$. Hence $f(x)=0$ and $F(V_1, x)=0$ have one common root x_1, and only one; if therefore we seek the common measure of $f(x)$ and $F(V_1, x)$, and continue the process till we obtain a remainder of the first degree in x, and equate that remainder to zero, we shall find $x_1=\phi_1(V_1)$. Next by fixing upon another root x_2 with a different coefficient in the expression of V, and going through the same process, we shall find $x_2=\phi_2(V_1)$, and so on.

Ex. To find the roots x_1, x_2, x_3 of $x^3 - 6x^2 + 11x - 6 = 0$, having given that a value of $V = x_1 + 2x_2 - 4x_3$ is 3.

The equation in V for determining x_1 is

$$(V - x_1 - 2x_2 + 4x_3)(V - x_1 - 2x_3 + 4x_2) = 0,$$

or $$(V - x_1)^2 + 2(x_2 + x_3)(V - x_1) + 20x_2x_3 - 8(x_2^2 + x_3^2) = 0.$$

But $x_1 + x_2 + x_3 = 6$, $x_2x_3 + x_1(x_2 + x_3) = 11$, $x_1^2 + x_2^2 + x_3^2 = 14$;

$$\therefore\ V^2 - 4Vx_1 + 12V + 31x_1^2 - 132x_1 + 108 = 0,$$

or, putting for V its given value 3,

$$31x_1^2 - 144x_1 + 153 = 0,$$

which is found to have a common measure $x_1 - 3$ with the proposed. Similarly, the equation in V for determining x_2 will be

$$(V - 2x_2 - x_1 + 4x_3)(V - 2x_2 - x_3 + 4x_1) = 0,$$

which may be reduced to

$$31x_2^2 - 159x_2 + 194 = 0,$$

and is found to have a common measure $x_2 - 2$ with the proposed. Also the equation for the remaining root will be found to be

$$31x_3^2 - 69x_3 + 38 = 0,$$

which has a common measure $x_3 - 1$ with the proposed.

Obs. Any symmetrical function of the roots has but one value, however the roots are interchanged amongst themselves; but a function of the roots not symmetrical may assume several values by interchanging the roots amongst themselves. Thus the linear function of the three roots a, b, c,

$$V = ma + nb + rc,$$

admits of six values; which we may form by taking along with abc, the other five permutations,

$$acb,\ bac,\ bca,\ cab,\ cba,$$

and substituting the letters of each in the same order in which they stand in it, in the expression for V. But if $n = r$,

so that V is symmetrical with respect to two of the roots, then V has only three distinct values; for the two values in which a stands first, become identical: and the same is true of the two values in which b stands first, and in which c stands first.

Lagrange has shewn, generally, that the number of distinct values which a function of n letters can assume by the permutations of the letters amongst themselves, when it falls short of $1.2.3 \ldots n$, is always a divisor of $1.2.3 \ldots n$.

The next step in the Problem would be to determine by which of those divisors in any given case, the number of values which a function of n letters admits of, is expressed; but at present the chief results which have rewarded the labours of Mathematicians in this inquiry, are the following: (1) that a function of n letters ($n > 4$), if it have fewer than n values, has at most two values; and (2) that a function of n letters (n different from 6), if it have exactly n values, is symmetrical with respect to $n-1$ of those letters. We are prepared for the exception $n=4$ in the first result, because we have already met with functions of four letters that admit of three values; and the exception $n=6$ in the second result arises from the circumstance that there are functions of six letters which have six distinct values, without being symmetrical relative to five of the letters. It is owing, as we know, to the fact of the existence of functions of three letters, such as $(a+\alpha b+\alpha^2 c)^3$ where $\alpha^3=1$, which have but two values; and of functions of four letters, such as $(a+b-c-d)^2$, which have but three values, that we are able to solve the general equations of the third and fourth degree. If we could form functions of five letters admitting of only four distinct values, we might expect to arrive, in the same way, at the solution of the general equation of the fifth degree; but a function of five letters, if it have fewer than five distinct values, has at most two values, so that, for the general equation of the fifth degree, it would be impossible to form a reducing equation of a degree inferior to the fifth.

Hence we perceive the important bearing which the research of the number of values that a rational function admits of, from permuting the letters of which it is composed, has upon the Theory of Equations.

It is always possible to form a function of n letters $a, b, c \ldots k, l$, which shall have but two values; for if from each of these letters we subtract all that follow it, and then take the product of all these differences, we shall find a function v of n letters

$$(a-b)(a-c)\ldots(a-l)(b-c)\ldots(k-l)$$

having only two values; for v^2 would be a symmetrical function of the n letters, and therefore would have but one value; and consequently v admits of only two values, equal to one another but of contrary signs. Hence if A and B represent any two symmetrical functions of the n letters $a, b, c \ldots l$, then the function $A + Bv$ will have only two values. The general form of a function of n letters having n values, is that it is symmetrical relative to $n-1$ of these letters.

QUADRATIC FACTORS OF EQUATIONS.

165. Every equation of an even degree has at least one real quadratic factor.

Let the proposed equation, having roots a, b, c, &c., be

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0;$$

and let $n = 2\mu$, μ being an odd number. Let it be transformed (Art. 162) into an equation whose roots are the combinations of every two of its roots, of the form $y = a + b + mab$, m being any number; also let the transformed equation be $\phi_m(y) = 0$; then its coefficients will be symmetrical functions of a, b, c, &c., and therefore rational and known functions of p_1, p_2, &c.; and its degree will be $\dfrac{2\mu(2\mu-1)}{2}$ which is odd; therefore

$\phi_m(y) = 0$ will have at least one real root, whatever be the value of m. Hence, making $m = 1, 2, 3, \ldots \{\mu(2\mu - 1) + 1\}$, successively, each of the equations $\phi_1(y) = 0$, $\phi_2(y) = 0$, &c., will have at least one real root; that is, we shall have $\mu(2\mu - 1) + 1$ real values for combinations of two roots of the proposed equation, of the form $a + b + mab$; but there are only $\mu(2\mu - 1)$ such combinations which are differently composed of the roots a, b, c, &c.; therefore two of these combinations, for which we have obtained real values, must involve the same pair of the quantities a, b, c, &c.; let this pair of roots be a, b, and α, α', the real roots of the corresponding equations $\phi_m(y) = 0$, $\phi_{m'}(y) = 0$, so that

$$a + b + mab = \alpha, \quad a + b + m'ab = \alpha';$$

therefore $a + b$ and ab are real, and the proposed equation has at least one real quadratic factor, and two roots, either real, or of the form $\alpha \pm \beta\sqrt{-1}$. Hence every equation whose degree is only once divisible by 2, has at least one real quadratic factor.

We shall now prove that if it be true that every equation has at least one real quadratic factor when its degree is r times divisible by 2, or when $n = 2^r\mu$ where μ is odd, the same is true when the degree of the equation is $r + 1$ times divisible by 2. For let $n = 2^{r+1}\mu$; then the degree of the transformed equation will be $2^r\mu(2^{r+1}\mu - 1)$, which is only r times divisible by 2; therefore, by supposition, the transformed equation, $\phi_m(y) = 0$, will have two roots, either real or imaginary. If they are real, then exactly in the same way as for the preceding case of the index being only once divisible by 2, it may be shewn that the proposed equation has at least one real quadratic factor. If they are imaginary, we shall have $y = \alpha \pm \beta\sqrt{-1}$, each of which quantities expresses the value of some one of the combinations

$$a + b + mab, \quad a + c + mac, \text{ \&c.}$$

Suppose therefore that we have $a + b + mab = \alpha + \beta\sqrt{-1}$: then, as shewn above, we can give m such a value m', that

$\phi_{m'}(y) = 0$ shall have a root corresponding to the combination of the same letters, so that $a + b + m'ab = \alpha' + \beta' \sqrt{-1}$, from which equations we can obtain values of ab and $a + b$ under the forms

$$a + b = \gamma + \delta \sqrt{-1},$$
$$ab = \gamma' + \delta' \sqrt{-1};$$

$$\therefore\ x^2 - (\gamma + \delta \sqrt{-1})\, x + \gamma' + \delta' \sqrt{-1} \text{ is a factor of } f(x);$$

but if any real expression have a factor of the form

$$M + N\sqrt{-1},$$

it must also have one of the form

$$M - N\sqrt{-1};$$

$$\therefore\ x^2 - (\gamma - \delta \sqrt{-1})\, x + \gamma' - \delta' \sqrt{-1} \text{ is a factor of } f(x);$$

if therefore these two expressions have no simple factor in common, their product will be a biquadratic factor of $f(x)$,

$$(x^2 - \gamma x + \gamma')^2 + (\delta x - \delta')^2,$$

which can always be resolved into two real quadratic factors (Art. 93).

If they have a factor in common, since they may be written

$$x^2 - \gamma x + \gamma' - \sqrt{-1}\,(\delta x - \delta'),\ \ x^2 - \gamma x + \gamma' + \sqrt{-1}\,(\delta x - \delta'),$$

it can only be of the form $x - \epsilon$; and the factors themselves become

$$(x - \kappa + \lambda \sqrt{-1})\,(x - \epsilon),\ \ (x - \kappa - \lambda \sqrt{-1})\,(x - \epsilon);$$

and therefore the proposed equation admits the real quadratic factor

$$(x - \kappa)^2 + \lambda^2.$$

Hence an equation whose degree $= 2^{r+1}\mu$ will have a real quadratic factor, provided an equation whose degree $= 2^r\mu$ has one; but we have proved this to be the case when $r = 1$; therefore it is universally true that every equation of an even degree has at least one real quadratic factor. If now this

factor be expelled, the depressed equation will have its coefficients real and its degree even, and will therefore, as before, have one real quadratic factor. Hence the first member of every equation of an even degree may be resolved into real quadratic factors.

166. Hence if we divide the first member of any equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \dots + p_n = 0$$

by $x^2 + ax + b$, admitting no terms into the quotient that have x in the denominator, we shall at last obtain a remainder of the form $Ax + B$, A and B being rational functions of a and b; and in order that $x^2 + ax + b$ may be a quadratic factor of the proposed equation, it is necessary and sufficient that this remainder should equal zero for all values of x, which requires that we separately have $A = 0$, $B = 0$. The different pairs of values real or imaginary of a and b which satisfy these equations, will give all the quadratic factors of the proposed; and as the number of these factors is $\frac{1}{2}n(n-1)$ (Art. 17), the final equation for determining one of the quantities a, b, obtained by eliminating the other between the two preceding equations, will be of the degree $\frac{1}{2}n(n-1)$, which exceeds n, if $n > 3$; therefore the determination of the quadratic factors of an equation will generally present greater difficulties than the solution of the equation.

As the proposed equation has necessarily $\frac{1}{2}n$ or $\frac{1}{2}(n-1)$ real quadratic factors, according as n is even or odd, there will always exist the same number of pairs of real values of a and b, satisfying the equations $A = 0$, $B = 0$; and if any of these pairs of real values be commensurable, they may be easily found; and the commensurable quadratic factors being known, the equation may be depressed.

Ex. 1. To resolve $x^4 - 6x^2 + nx - 3 = 0$ into its factors. Dividing by $x^2 + ax + b$, we find a remainder

$$(n + 2ab + 6a - a^3)\,x - (a^2b - b^2 - 6b + 3);$$

therefore, to determine a and b, we have

$$n + 2ab + 6a - a^3 = 0,$$
$$a^2b - b^2 - 6b + 3 = 0.$$

Solving the former with respect to b, and substituting in the latter, we find $(a^2 - 4)^3 = n^2 - 64$, or $a = \sqrt{4 + \sqrt[3]{n^2 - 64}}$; from whence b, and the other quadratic factor

$$x^2 - ax + a^2 - b - 6,$$

may be determined.

Ex. 2. To resolve $x^4 + px^3 + qx^2 + rx + s$ into its two quadratic factors

$$x^2 + mx + n, \quad x^2 + m'x + n'.$$

Since $-p = a + b + c + d$, the sum of any two roots is not, in this case, equal to the sum of the other two with a contrary sign; and therefore the equation for determining

$$m = -(a + b)$$

would rise to the sixth degree. But we have

$$2m - p = -(a + b) + c + d,$$

a function of the roots the six values of which are equal two and two and of opposite signs, and which we may denote by $z^{\frac{1}{2}}$; then z is determinable by a cubic equation, and the resolution may be effected by the following formulæ:

$$m = \tfrac{1}{2}(p + \sqrt{z}), \qquad m' = \tfrac{1}{2}(p - \sqrt{z}),$$

$$n = \frac{r - qm + pm^2 - m^3}{p - 2m}, \quad n' = \frac{r - qm' + pm'^2 - m'^3}{p - 2m'},$$

where z is a root of the equation (which has necessarily a real root)

$$z^3 - (3p^2 - 8q)z^2 + (3p^4 - 16p^2q + 16q^2 + 16pr - 64s)z$$
$$- (8r - 4pq + p^3)^2 = 0.$$

EVERY ALGEBRAIC EQUATION HAS A ROOT.

167. There is no uncertainty about the existence of a real root for every equation, except for an equation of an even

degree with its last term positive; an equation of this sort may not admit of any real root, but then it must have an imaginary root; and we are now able to supply a proof of what was assumed at Art. 11, namely that every equation has a root, in the following Theorem; the truth of which, at least for equations with real coefficients, may be considered to have already been established in the foregoing Proposition of Art. 165.

An equation of any degree with coefficients either real or imaginary, has always at least one root of the form $a + b\sqrt{-1}$, where a and b are real finite quantities, but either of them may be zero.

We must first prove that this is true with regard to the binomial equations

$$x^n = \pm 1, \quad x^n = \pm \sqrt{-1},$$

to which the more general forms $x^n = \pm c$, $x^n = \pm c\sqrt{-1}$ may easily be reduced.

The equation $x^n = 1$ is always satisfied by $x = 1$, and the equation $x^n = -1$, when n is an odd number, by $x = -1$; the other cases of both equations are included in the solution of

$$x^n = +\sqrt{-1};$$

for suppose we have found a value $x = \alpha$, which satisfies this equation: then since

$$\alpha^n = +\sqrt{-1}, \quad \alpha^{2n} = (\alpha^2)^n = -1, \quad \text{and } \alpha^{3n} = (\alpha^3)^n = -\sqrt{-1};$$

so that α^2 and α^3 are, respectively, roots of

$$x^n = -1, \text{ and of } x^n = -\sqrt{-1}.$$

It is therefore only necessary to consider the equation

$$x^n = +\sqrt{-1};$$

if n be odd, n is of one of the forms $4m + 1$, or $4m + 3$; and the equation is satisfied by $x = +\sqrt{-1}$ in the first case, and by $-\sqrt{-1}$ in the second; if n be even, and equal to $2n'$ where n' is odd, then, putting $x^2 = y$, the proposed equation is replaced by $y^{n'} = +\sqrt{-1}$, which, as n' is odd, admits of a root

$\pm\sqrt{-1}$; and then two values of x can be obtained under the form $a+b\sqrt{-1}$ by extracting the square root of $\pm\sqrt{-1}$ after the ordinary method. Similarly, if $n=2^{r+1}\times n'$, where n' is odd, putting $x^2=y$, the equation is replaced by $y^{2^r.n'}=+\sqrt{-1}$; and if this give a value of y under the form $a+b\sqrt{-1}$, we get, by extracting the square root, two values of x under the same form. But if $r=1$, we have proved that $x^{2n'}=+\sqrt{-1}$ admits of a solution of the form $a+b\sqrt{-1}$; therefore $x^n=+\sqrt{-1}$ always admits of a solution of the same form, n being any even or odd number.

Next let us consider the general case of

$$f(x)=x^n+p_1x^{n-1}+\ldots+p_n=0,$$

the coefficients being real or imaginary. If in it for x we substitute $a+b\sqrt{-1}$, where a and b are real quantities, the first number will assume the form $A+B\sqrt{-1}$, A and B denoting real quantities functions of a and b; and in order that $a+b\sqrt{-1}$ may be a root of the proposed, we must have $A=0$, $B=0$, or we must have the modulus of $A+B\sqrt{-1}$, viz. $\sqrt{A^2+B^2}=0$. Let us suppose that this condition is not satisfied; we shall shew that a corrected value of the same form, can be given to x such that the result of the substitution of this new value will have a modulus smaller than $\sqrt{A^2+B^2}$ the modulus of the first result. To this end assume

$$x=a+b\sqrt{-1}+eu,$$

where e denotes a number as small as we please, and u an indeterminate quantity which may receive either real or imaginary values. If in the development of $f(x+h)$

$$=f(x)+hf'(x)+\tfrac{1}{2}h^2f''(x)+\ldots+h^n\ldots(1)$$

we put $x=a+b\sqrt{-1}$, and $h=eu$,

$f(x)$ will become $A+B\sqrt{-1}$; some of the coefficients of the powers of h may vanish by this substitution, but not all of

them, since the coefficient of h^n is unity. Let h^r be the lowest power of h which does not vanish, and $R + S\sqrt{-1}$ its coefficient, where R and S are not equal to zero at the same time.

Calling therefore the result of the substitution in $f(x)$ of

$$a + b\sqrt{-1} + eu \text{ for } x, \ A' + B'\sqrt{-1},$$

we get

$$A' + B'\sqrt{-1} = A + B\sqrt{-1} + (R + S\sqrt{-1})(eu)^r + \text{terms in } (eu)^{r+1} \dots (eu)^n \ (2).$$

Now as $u^r = c$ always admits of a root of the form

$$\alpha + \beta\sqrt{-1},$$

we may suppose u^r to be a real quantity c; therefore, substituting for u its value, and equating to one another the real and imaginary parts of (2), we find

$$A' = A + Rce^r + \text{real terms in } e^{r+1} \dots e^n,$$

$$B' = B + Sce^r + \text{real terms in } e^{r+1} \dots e^n.$$

Consequently, the square of the modulus of $A' + B'\sqrt{-1}$ is

$$A'^2 + B'^2 = A^2 + B^2 + 2(AR + BS)ce^r + \text{real terms in } e^{r+1} \dots e^{2n}.$$

Now we may assume the number e so small that the aggregate of the terms that follow $A^2 + B^2$ may take the sign of the term $2(AR + BS)ce^r$; and we may always render this last term negative by taking $c = +1$ or -1 according as $AR + BS$ is negative or positive. When these conditions relative to e and c are satisfied, we have

$$A'^2 + B'^2 \text{ less than } A^2 + B^2.$$

This demonstration requires that $AR + BS$ must not $= 0$; if this should be the case, then, as $u^r = c\sqrt{-1}$ always admits of a root of the form $\alpha + \beta\sqrt{-1}$, we may assume u^r to be an imaginary quantity $c\sqrt{-1}$; therefore, substituting for u its value and equating to one another the real and imaginary parts of (2) as before, we get

$$A' = A - Sce^r + \&c.,\quad B' = B + Rce^r + \&c.;$$
$$\therefore\ A'^2 + B'^2 = A^2 + B^2 - 2\,(AS - BR)\,ce^r + \&c.,$$

the terms which follow being real, and containing no power of e inferior to r. Since $AR + BS = 0$, we cannot have also $AS - BR = 0$; for if these coexist, then we find the sum of their squares or $(A^2 + B^2)(R^2 + S^2) = 0$, which resolves itself into either $A = 0$, $B = 0$; or $R = 0$, $S = 0$; contrary to the suppositions that have been made. The quantity $AS - BR$ being different from zero, we may, as before, assume e so small that the term involving e^r shall exceed the aggregate of all the succeeding terms; and that term may be rendered negative by assuming $c = +1$, or -1, according as $AS - BR$ is positive or negative. Consequently, when the two conditions relative to e and c are satisfied we still find $A'^2 + B'^2$ less than $A^2 + B^2$.

If therefore $\sqrt{A^2 + B^2}$, the modulus of the result of substituting $a + b\sqrt{-1}$ for x in $f(x)$, does not vanish, we may, by assigning suitable values to u and e, obtain a corrected value of $x = a + b\sqrt{-1} + cu$, such that $\sqrt{A'^2 + B'^2}$, the modulus of the result of substituting it in $f(x)$, may be less than $\sqrt{A^2 + B^2}$. Hence it follows that there must exist a value of x of the form $a + b\sqrt{-1}$ such that, upon substituting it in the proposed equation, we shall eventually obtain a result whose modulus is zero; such a value is a root of the equation. And in this value of x the quantities a and b are finite; as we shall establish by shewing that the result of the substitution cannot be a finite quantity unless a and b be finite. For representing as before the result of the substitution of $a + b\sqrt{-1}$ for x in $f(x)$ by $A + B\sqrt{-1}$, we get

$$A + B\sqrt{-1} = (a + b\sqrt{-1})^n \left\{1 + \frac{p_1}{a + b\sqrt{-1}} + \ldots + \frac{p_n}{(a + b\sqrt{-1})^n}\right\}.$$

Now the real or imaginary quantities $p_1, p_2 \ldots p_n$ have each a finite modulus; if therefore we suppose the quantities a and b, or one of them, to increase indefinitely, the modulus

of each of the fractions $\frac{p_1}{a+b\sqrt{-1}}$, &c., will decrease indefinitely; and these fractions will become

$$\alpha_1 + \beta_1\sqrt{-1},\ \ \alpha_2 + \beta_2\sqrt{-1},\ \&c.,$$

where the quantities α_1, β_1, &c. may be as small as we please; for any one of them, by Art. 85, admits of the transformation

$$\frac{p_m}{(a+b\sqrt{-1})^m} = \frac{\rho\,(\cos\phi + \sqrt{-1}\sin\phi)}{r^m\,(\cos m\theta + \sqrt{-1}\sin m\theta)}$$

$$= \frac{\rho}{r^m}\{\cos(\phi - m\theta) + \sqrt{-1}\sin(\phi - m\theta)\}.$$

Consequently the factor of $(a+b\sqrt{-1})^n$ will be reduced to an expression of the form $1+\gamma+\delta\sqrt{-1}$, where γ and δ may be as small as we please; and the modulus of this factor $\sqrt{(1+\gamma)^2+\delta^2}$ will approach indefinitely near to unity. But the modulus of $(a+b\sqrt{-1})^n$ will increase indefinitely; therefore the modulus of $A+B\sqrt{-1}$ will itself increase indefinitely.

Without therefore assigning the value of the root, and without examining whether there exist several values of x which make $f(x)=0$, we may at all events conclude, from the above investigation, that an equation of any degree, with either real or imaginary coefficients, has necessarily one root of the form $a+b\sqrt{-1}$; where a and b are real finite quantities, but either of them may be zero.

SECTION IX.

ON ELIMINATION.

---

168. An equation between two unknown quantities x and y, supposed to contain no term which is fractional or irrational, is said to be of the degree which is expressed by the sum of the indices of x and y in that term where the sum is the greatest. The general equation of the n^{th} degree between x and y ought to contain all the terms in which the sum of the indices does not exceed n; therefore, when complete and arranged according to descending powers of x, it will be

$$a_0x^n + (b_0 + b_1y)\,x^{n-1} + (c_0 + c_1y + c_2y^2)\,x^{n-2} + \ldots$$
$$+ (l_0 + l_1y + l_2y^2 + \ldots + l_ny^n) = 0.$$

When an equation is incomplete, that is, when it does not contain all the terms which belong to its degree, we must suppose, in the general equation, the coefficients of the deficient terms to be equal to zero.

Although we are always at liberty to divide an equation by any one of its coefficients, we cannot in the above general equation suppose $a_0 = 1$, for then it would not comprehend those equations which want the term involving x^n. After having divided the equation by any one of its coefficients, there will remain as many indeterminate constants as there are terms, wanting one; the number of these constants will therefore be

$$2 + 3 + 4 + \ldots + (n+1) = \tfrac{1}{2}n\,(n+3),$$

which expresses how many conditions an equation of the n^{th} degree may be made to satisfy, by a suitable determination of its coefficients.

To eliminate between two equations of any degree involving two unknown quantities, is to obtain an equation containing only one of the unknown quantities, and which gives all the values of this unknown quantity, which, together with the corresponding values of the other unknown, can satisfy the proposed equations. This equation, involving only one unknown quantity, is called the final equation, and its roots are called suitable values.

In what follows, we shall suppose the polynomials which form the first members of the equations to be freed from any common divisor which they may admit; for if they had a common divisor containing both variables, it might be reduced to zero, and therefore the proposed equations might be satisfied, by an infinite number of systems of values of x and y; or if they had a common divisor containing only one of the variables, there would be a limited number of values of that variable, and an unlimited number of values of the other, by which the proposed equations might be satisfied; sc that in both cases there could be no final equation.

METHOD OF ELIMINATION BY THE GREATEST COMMON MEASURE.

169. To determine all the systems of values which will satisfy two equations between two unknown quantities, each being of any degree.

Let $F(x, y) = 0$, $f(x, y) = 0$, be two equations, respectively of the m^{th} and n^{th} degrees, admitting only a limited number of pairs of values of x and y, and their first members consequently having no common divisor, involving either both or only one of the variables. Then in order that any value $y = \beta$, may be a suitable value, it is necessary that there should exist one or more values of x which, substituted in the polynomials $F(x, \beta), f(x, \beta)$, will reduce them to zero; these polynomials must therefore have a common measure a function of x, which, equated to zero, will give one or more values

of x, that, jointly with $y=\beta$, satisfy the proposed equations. If therefore we perform the operation for finding the greatest common measure of $F(x, y)$, $f(x, y)$, (which we suppose arranged according to descending powers of x) introducing or suppressing factors, functions of y, so that no quotient shall have any term with y in its denominator, we shall at last arrive at a remainder independent of x, which put equal to zero will give the final equation $\psi(y)=0$. For if β be a root of this equation, and $\phi(x, y)$ be the last divisor, since $y=\beta$ makes the remainder vanish, $\phi(x, \beta)$ is a common measure of the polynomials $F(x, \beta)$, $f(x, \beta)$; therefore $\phi(x, \beta)=0$ will give values of x which, jointly with $y=\beta$, satisfy the proposed equations.

OBS. In those cases where the process for the common measure requires neither the introduction nor suppression of factors, we are certain that the last remainder put equal to zero, or $\psi(y)=0$, will furnish all the suitable values of y, and no more; but we cannot affirm this in other cases, unless we are certain that the last remainder is unaffected by the factors that have been rejected or introduced; and it frequently happens that in the final equation, values of y are found which are foreign to the problem, and others are deficient which belong to it. On this account the method of elimination by the greatest common measure is imperfect, but it is still the most convenient practical one for numerical equations.

170. In particular cases we are able to find all the systems of values which satisfy two proposed equations, by easier methods than the one just described.

Thus, whenever we are able to solve one of the equations with respect to one of the unknown quantities, x for instance, we have only to substitute the resulting expressions for x in the other equation, and we shall obtain equations containing y only; and if we substitute the values of y given by these equations in the corresponding expressions for x, we shall obtain all the pairs of values required. Also, if the two equations

are of the same degree with respect to the variable which we wish to eliminate, we may, by introducing factors, if necessary, and subtracting, depress one of them to an inferior degree. And if the first members of the equations are, or can be, resolved into their factors, then the solution of them is reduced to the simpler case of finding all values of x and y which reduce at the same time a factor of each to zero.

171. In all cases of elimination between the equations

$$F(x, y) = 0, \quad f(x, y) = 0,$$

besides expelling any common factor which the polynomials admit, the application of the general method may be simplified by previously ascertaining whether either has factors containing only one of the variables.

This may be done by arranging each, first according to powers of y, and finding the greatest common measure of the coefficients of the several powers of y in it; and secondly by arranging each according to powers of x, and finding the greatest common measure of the coefficients of the several powers of x. Let X, Y, be the factors thus discovered of $F(x, y)$, and M its remaining factor; and let X', Y', N, be similar quantities for $f(x, y)$; then the proposed system may be replaced by

$$XYM = 0, \quad X'Y'N = 0,$$

which will be satisfied by simultaneously putting any factor of each equal to zero, provided we do not take X and X' together, or Y and Y' together; for X and X' cannot be reduced to zero by the same value of x, unless they have a common factor; and that they cannot have, since by the supposition $F(x, y)$, $f(x, y)$, have no common factor. Hence, with the exception of $M = 0$, $N = 0$, each of the systems into which the system $F(x, y) = 0$, $f(x, y) = 0$, is resolved, has at least one of its equations involving only one unknown quantity; and therefore its solution is attended with no other difficulties than what belong to equations of that description. But the system $M = 0$, $N = 0$, whose first members contain

both variables, but have no factors depending on x only, or y only, will require the process of elimination by the greatest common measure to be applied to them, in order to reduce their solution to that of equations containing only one unknown quantity, as we shall now more minutely explain.

172. To examine the consequences of introducing or suppressing factors in the process of elimination by the greatest common measure, and to investigate the means of obtaining an exact final equation.

Let $M=0$, $N=0$, be two equations between x and y, of the m^{th}, and n^{th} degree, respectively; the polynomials M and N being arranged according to descending powers of x, and not admitting a common divisor, and neither of them having a factor composed of x only, or of y only; and let m be greater than n. Divide M by N, and let Q be the quotient (containing no term with y in its denominator) and R the remainder, so that

$$M = QN + R;$$

then all values of x and y which satisfy $M=0$, $N=0$, also satisfy $N=0$, $R=0$; but if the division cannot be performed without putting powers of y in the denominator of the quotient, i.e. if Q be of the form $\frac{H}{K}$, where K contains y, then we cannot affirm that all values which satisfy the proposed system, also satisfy $N=0$, $R=0$; for the equation

$$M = \frac{H}{K}.N + R$$

shews that values which make $M=0$, $N=0$, may make $K=0$, so that $\frac{H}{K}.N$ may assume the form $\frac{0}{0}$, the real value of which, and therefore of R, may be finite or infinite, instead of zero; and, conversely, values which make $N=0$, $R=0$, may still not make the second member equal to zero, and therefore not make M equal to zero. To avoid fractional

quotients, we must use the same means as in finding the greatest common measure; that is, we must multiply M by the coefficient of the first term of N, or by certain factors of that coefficient; then no common factor will have been introduced into both polynomials; and if P, a function of y, represent this multiplier, Q the quotient, and R the remainder, we shall have

$$PM = QN + R,$$

which shews that the solutions of $N=0$, $R=0$, are the same as those of $PM=0$, $N=0$. But these latter equations resolve themselves into the two systems

$$M=0,\ \ N=0;\ \ P=0,\ \ N=0.$$

Therefore, besides furnishing the solutions of the proposed equations, the system $N=0$, $R=0$, will furnish those of $P=0$, $N=0$. Hence we must solve the two latter equations, one of which $P=0$ contains only y, and substitute all the resulting pairs of values of x and y in $M=0$: then those pairs of values which do not satisfy it must be rejected, and we shall thus obtain those solutions of $N=0$, $R=0$, which belong to the proposed system $M=0$, $N=0$.

The remaining solutions of the proposed system are contained in the equations $N=0$, $R=0$, R being a polynomial of smaller dimensions than N. Now if R have factors containing only one of the variables, (which may be discovered by seeking the greatest common measure of its coefficients, when arranged according to the powers of each variable in succession,) so that $R = XYR'$, then the system $N=0$, $R=0$, may be resolved into the three systems,

$$N=0,\ \ X=0;\ \ N=0,\ \ Y=0;\ \ N=0,\ \ R'=0;$$

the two former of which present no difficulty, because one equation in each contains only one variable; and the third $N=0$, $R'=0$, is exactly of the same nature as the one we started with; for N, R', have no common factor, otherwise M and N would have the same common factor, which is contrary to the supposition, and neither N nor R' admits a

factor containing only one of the variables. This system then, by exactly the same process, may be replaced by another similar system $R'=0$, $R''=0$, the latter being of a lower degree in x than the former; and the system $R'=0$, $R''=0$, by another, of which the second equation will be of a degree in x, inferior to that of $R''=0$. In continuing these uniform operations, we shall at last arrive at a remainder not containing x; suppose this to be R'', then the solution of the proposed system is reduced to that of $R'=0$, $R''=0$, and is thus made to depend upon the solution of an equation containing only one unknown quantity.

173. In ascending from $R'=0$, $R''=0$, to the preceding system $N=0$, $R'=0$, it may happen that some solutions will have to be added, and others suppressed; and, similarly, in ascending from $N=0$, $R'=0$, to $M=0$, $N=0$; and so on, if there were a greater number of successive divisions. This method then, as we perceive, will not always lead to a single equation in y, but to several, some of which may give unsuitable values for that variable. When we have recognized all those which really enter into the solutions common to the two proposed equations, we may, if necessary, combine them into one final equation.

It may be observed that, since M and N are prepared so as to admit no common measure, we can never find zero, but we may find a number, for the last remainder R''; in that case, the final equation, $R''=0$, is absurd; and the proposed equations (unless solutions have been suppressed in the process) are incompatible with one another; i. e. incapable of being satisfied by finite values of x and y. It is easy to form equations of this sort; such for instance are $P=0$, $PQ+k=0$; P and Q being integral functions of x and y, and k a number; for the condition expressed by the former, reduces the latter to $k=0$, which is absurd, since k is a number.

Also from the final equation $R''=0$, we can never deduce a value β, of y, which will reduce the preceding divisor R'

to zero independently of the value of x; for in that case, R' would have a factor, $y-\beta$, which is impossible, because in the process each remainder, before being employed as a divisor, is cleared of factors containing x only, or y only; but $y=\beta$ may destroy some of the terms in R', and so cause $R'=0$ to furnish a greater or smaller number of corresponding values of x, or none at all if $y=\beta$ reduce R' to a number. Of the above peculiarities, and of the application of the general method, the following are instances:

*Ex. 1.
$$yx^3-(y^3-3y-1)x+y=0,$$
$$x^2-y^2+3=0.$$

The first division gives the remainder $x+y$; and the division of x^2-y^2+3 by $x+y$ gives the remainder 3. The proposed equations are therefore incompatible.

Ex. 2.
$$(y-1)x^3+(y^2+y)x^2+(3y^2+y-2)x+2y=0,$$
$$(y-1)x^2+(y^2+y)x+3y^2-1=0.$$

The final equations are
$$y^2-1=0,\quad (y-1)x+2y=0;$$
the former gives $y=\pm 1$; but the value $y=1$, furnishes no corresponding finite value of x, since it reduces the latter to $2=0$.

Ex. 3.
$$x^3-3yx^2+(3y^2-y+1)x-y^3+y^2-2y=0,$$
$$x^2-2yx+y^2-y=0.$$

$$
\begin{array}{r}
x^2-2yx+y^2-y\,\big)\,x^3-3yx^2+(3y^2-y+1)x-y^3+y^2-2y\,\big(x-y \\
\underline{x^3-2yx^2+(y^2-y)x\qquad\qquad\qquad} \\
-yx^2+(2y^2+1)x-y^3+y^2-2y \\
\underline{-yx^2+2y^2x-y^3+y^2\qquad} \\
x-2y\,\big)\,x^2-2yx+y^2-y\,\big(x \\
\underline{x^2-2yx\qquad\quad} \\
y^2-y,
\end{array}
$$

therefore the final equations are

$$x - 2y = 0, \quad y^2 - y = 0,$$

$$\text{which give } \left.\begin{matrix} y = 0 \\ x = 0 \end{matrix}\right\} \quad \left.\begin{matrix} y = 1 \\ x = 2 \end{matrix}\right\};$$

and as no factor has been introduced or suppressed, these two solutions are those of the proposed system.

Ex. 4. $$(y-2)\,x^2 - 2x + 5y - 2 = 0,$$
$$yx^2 - 5x + 4y = 0.$$

Multiplying the dividend by y,

$$yx^2 - 5x + 4y \,\big)\; (y-2)\,yx^2 - 2yx + 5y^2 - 2y \;\big(\, y - 2$$
$$\underline{(y-2)\,yx^2 - (5y-10)\,x + 4y^2 - 8y}$$
$$(3y-10)\,x + y^2 + 6y.$$

Next multiplying the dividend by $(3y-10)^2$,

$$(3y-10)\,x + y^2 + 6y \,\big)$$
$$(3y-10)^2yx^2 - 5\,(3y-10)^2x + 4\,(3y-10)^2y \;\big(\,(3y-10)\,yx - \&c.$$
$$\underline{(3y-10)^2yx^2 + (3y-10)\,(y^2+6y)\,yx}$$
$$-(3y-10)\,(y^3 + 6y^2 + 15y - 50)\,x + 4\,(3y-10)^2y$$
$$\underline{-(3y-10)\,(y^3 + 6y^2 + 15y - 50)\,x - (y^2+6y)\,(y^3 + 6y^2 + 15y - 50)}$$
$$y^5 + 12y^4 + 87y^3 - 200y^2 + 100y.$$

Therefore the final equations are (suppressing the factor y, since the solution $y = 0, x = 0$, does not satisfy the proposed system, and is due to the factor introduced in the operation)

$$(3y-10)\,x + y^2 + 6y = 0,$$
$$y^4 + 12y^3 + 87y^2 - 200y + 100 = 0,$$

which contain no false values; for the only false value which the final equation in y could contain, would be $\frac{10}{3}$, which is

impossible, since all the coefficients of that equation are integers. One pair of values is $y=1$, $x=1$; the other solutions can be obtained only approximately.

Ex. 5.
$$x(4y^2+3)-8ay=0,$$
$$4y(3-2x^2)-4y^2+3=0.$$

Here we can solve with respect to one of the variables, and we find for the final equations

$$(x^2-1)^3=a^2-1,\ \ y=\frac{a}{x}+\frac{3}{2}-x^2;$$
$$\therefore\ x=\sqrt{1+\sqrt[3]{a^2-1}},$$
$$y=\frac{a}{\sqrt{1+\sqrt[3]{a^2-1}}}+\tfrac{1}{2}-\sqrt[3]{a^2-1}.$$

Ex. 6.
$$y=\phi(x),\ \ x=\phi(y).$$

The final equation resulting from the elimination of either of the variables between simultaneous equations of this form, admits of a remarkable reduction. For, suppose a to be a root of $x-\phi'(x)=0$, and put $x=y=a$ in the proposed system of equations; then they are evidently satisfied; therefore $x=a$ satisfies the final equation

$$x=\phi\{\phi(x)\},\ \text{or}\ f(x)=0;$$

therefore every factor of $x-\phi(x)$ is a factor of $f(x)$;

$$\therefore\ f(x)=\{\phi(x)-x\}\,.f_1(x),$$

which leads to the reduced final equation $f_1(x)=0$.

Thus, let the system of equations be

$$y=\frac{16x(1-x)^2}{(1+x)^4},\ \ x=\frac{16y(1-y)^2}{(1+y)^4};$$

then

$$x(1+x)^4-16x(1-x)^2=x(x^2-2x+5)(x^2+6x-3)$$

is a factor of the final equation.

174. It was observed (Art. 23) that the problem of transforming an equation, in its widest sense, required the general

methods of elimination. This is especially the case where each root of the new equation is to be composed of several roots of the primitive equation. Of this use of the methods of elimination we shall now give some instances.

To transform an equation into one whose roots shall be the differences of every two roots of the proposed equation.

Let $f(x) = 0$ be an equation of n dimensions, having roots $a, b, c, \ldots l$; to obtain another equation whose roots are the differences between all the roots of the proposed and a, we must make $y = x - a$ or $x = a + y$, and the substitution of this value for x in $f(x) = 0$, will give $f(a+y) = 0$, the required equation; or, developing (Art. 27),

$$f(a) + f'(a) \cdot y + f''(a) \frac{y^2}{1 \cdot 2} + \ldots + y^n = 0 \ldots\ldots\ldots (1).$$

Since, by the supposition, a is a root of the proposed, $f(a) = 0$; therefore the preceding equation has y for a factor, or admits a root zero, corresponding to the difference $a - a$; suppressing this factor, we have

$$f'(a) + f''(a) \frac{y}{1 \cdot 2} + \ldots + y^{n-1} = 0 \ldots\ldots\ldots\ldots (2),$$

an equation having for its roots the difference between a and the $n-1$ other roots of the proposed equation. If in this equation we replace a by b, c, &c., successively, we shall form equations whose roots are the differences between b and the $n-1$ other roots, between c and the $n-1$ other roots, and so on. Hence it follows that the differences of every two of the roots of the proposed equation are the values of y furnished by the equation

$$f'(x) + f''(x) \frac{y}{1 \cdot 2} + \ldots + y^{n-1} = 0,$$

when we substitute successively in it, for x, all the roots of the equation $f(x) = 0$; which amounts to solving the system

formed by the above equation, and $f(x)=0$. If therefore we eliminate x between the equations

$$f(x)=0,\ f'(x)+f''(x).\frac{y}{1.2}+\ldots+y^{n-1}=0,$$

the resulting equation in y will be the one required. The proposed equation being of the n^{th} degree, the transformed equation will be of the $n(n-1)^{th}$ degree; for the number of its roots is equal to the number of permutations which can be formed with the n quantities $a, b, c, \ldots l$, taken two and two together; also the transformed equation will contain only even powers of y, for if it have a root $a-b$ it will also have the root $b-a$; so that its roots are equal two and two, and of contrary signs. Hence if $n(n-1)=2m$, and $y^2=z$, the transformed equation will be of the form

$$z^m+q_1z^{m-1}+q_2z^{m-2}+\ldots+q_m=0,$$

and the values of z are the squares of the differences of every two roots of the proposed equation.

Ex. $$x^3+qx+r=0.$$

In this case $f'(x)+f''(x).\frac{y}{1.2}+y^2=0$ gives

$$3x^2+q+3xy+y^2=0.$$

$$3x^2+3xy+y^2+q\,\big)\ 3x^3+3qx+3r\ \big(x-y$$

$$\frac{3x^3+qx+\ldots}{2(y^2+q)x+y^3+qy+3r}$$

$$2(y^2+q)x+y^3+qy+3r\,\big)$$

$$6(y^2+q)^2x^2+6(y^2+q)^2yx+2(y^2+q)^3\ \big(3x(y^2+q)+\ldots$$

$$\frac{6(y^2+q)^2x^2+3(y^2+q)^2yx+\ldots}{4(y^2+q)^3-3(y^3+qy+3r)(y^3+qy-3r)}$$

therefore, equating the last remainder to zero (since the factor y^2+q put equal to zero, reduces the last divisor to $3r$, which is different from zero), we have the equation of differences

$$y^6+6qy^4+9q^2y^2+4q^3+27r^2=0;$$

and putting $y^2=z$, the equation of the squares of the differences is (as at p. 45)

$$z^3+6qz^2+9q^2z+4q^3+27r^2=0.$$

By similar reasoning it may be shewn, that to transform $f(x)=0$, into one whose roots shall be the sum, product, or ratio of every two of its roots, we must eliminate x between $f(x)=0$, and

$$f'(x)+f''(x)\frac{h}{1.2}+\ldots+h^{n-1}=0,$$

where $h=y-2x$, $\frac{y}{x}-x$, and $xy-x$, respectively; taking in the two former cases the square root of the result.

175. To eliminate one of the unknown quantities between two equations containing two unknown quantities, by means of symmetrical functions.

Let $x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots+p_n=0$ .... (1)

$x^m+q_1x^{m-1}+q_2x^{m-2}+\ldots+q_m=0$ .... (2)

be two equations respectively of n and m dimensions in x and y; so that $p_1, p_2, \ldots p_n$ are functions of y involving respectively no power of y above the first, second, &c., n^{th}; and $q_1, q_2, \ldots q_m$ functions of y involving no power of y above the first, second, &c., m^{th}. If we can solve the first with respect to x, and deduce n values, a, b, c, &c., functions of y, then upon substituting them in the second, we shall have, for determining y, n equations not containing x, viz.

$$\left.\begin{array}{l} a^m+q_1a^{m-1}+q_2a^{m-2}+\ldots+q_m=0 \\ b^m+q_1b^{m-1}+q_2b^{m-2}+\ldots+q_m=0 \\ c^m+q_1c^{m-1}+q_2c^{m-2}+\ldots+q_m=0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots=. \end{array}\right\}\ldots\ldots\ldots (3).$$

But in general the solution of (1) is impossible, and our object must be to obtain a final equation containing indifferently all the suitable values of y, and this we shall do by multiplying together the above n equations; for the result will be satisfied by every value of y derived from any one of them, and by no other quantity; and to every one of these values of y there will correspond a value of x such that the pair will jointly satisfy (1) and (2). For suppose a value of y deduced from the first of equations (3) to be β, and let the equation $x-a=0$ give, by making $y=\beta$, $x=\alpha$; then it is manifest that $x=\alpha$, $y=\beta$, will jointly satisfy the proposed equations. But in the result of this multiplication, the factors only change places when we interchange in any manner the quantities a, b, c, &c.; therefore the product will only involve rational and integral symmetrical functions of these quantities, which may be expressed by means of the coefficients of equation (1); and we shall so obtain the final equation in y. The calculations required by this method are in general tedious; but it has the recommendation of giving the final equation with all the roots it ought to contain, and no others.

176. When we eliminate one of the unknown quantities between two equations containing two unknown quantities, the degree of the final equation cannot exceed the product of the degrees of the two equations between which the elimination is performed.

To prove this, we must examine to what degree y may rise in the symmetrical functions composing the product of equations (3). Each term of this product will be itself the product of terms, one taken out of each of the equations (3), and will therefore be of the form

$$q_{m-h}a^h \times q_{m-k}b^k \times q_{m-l}c^l \dots, \text{ or } q_{m-h} \times q_{m-k} \times q_{m-l} \dots \times a^h b^k c^l \dots$$

But the product of the n equations, being symmetrical, must contain all the terms of the same form which we can

make with the above quantities; consequently it will contain all the terms represented by

$$q_{m-h}q_{m-k}q_{m-l}\dots \Sigma(a^h b^k c^l \dots) \dots\dots\dots (4),$$

and we must now ascertain the dimensions of this expression.

Now the degree of y in q_{m-h}, q_{m-k}, &c. cannot exceed $m-h$, $m-k$, &c., respectively; therefore in $q_{m-h}\,q_{m-k}\,q_{m-l}\dots$ it will at most be equal to $mn-h-k-l-$&c. Also if we refer to the formulæ which give the values of the double, triple, &c. functions in terms of the sums of the powers of the roots, we see that in $\Sigma(a^h b^k c^l \dots)$ the term of highest dimension in y will be found in $S_h S_k S_l \dots$, but the equations which give S_1, S_2, &c., in terms of p_1, p_2, &c., (since these quantities do not involve powers of y exceeding the first, second, third, &c. respectively) shew that the degree of y in any sum S_h cannot exceed h; therefore the degree of y in $\Sigma(a^h b^k c^l \dots)$ cannot surpass $h+k+l+$&c.; consequently, in the expression (4), the degree of y will at the most be equal to mn. The same thing may be similarly proved of all the symmetrical functions whose sum makes up the product of the n equations. Therefore, lastly, the degree of the final equation cannot exceed the product of the degrees of the two equations from which it results by the elimination of one of the unknown quantities.

Although the degree of the final equation cannot exceed mn, in particular cases it may be less than mn. If we extend the process to any number of equations, we shall have the general theorem discovered by *Bezout*, viz. that if between equations equal in number to the unknown quantities, we eliminate all except one, the degree of the final equation will be at most equal to the product of the degrees of the several equations.

Ex. To eliminate x between the equations

$$yx^2 - 5x + 4y = 0,$$

$$(y-2)\,x^2 - 2x + 5y - 2 = 0.$$

Let a and b denote the values of x given by the first equation; then substituting them in the second equation, we have

$$(y-2)\,a^2 - 2a + 5y - 2 = 0,$$
$$(y-2)\,b^2 - 2b + 5y - 2 = 0;$$

the product of these equations, which will be the required final equation in y, is

$$(y-2)^2\,\Sigma(a^2b^2) - 2\,(y-2)\,\Sigma(a^2b) + (y-2)\,(5y-2)\,S_2$$
$$-\,2\,(5y-2)\,S_1 + 4\,\Sigma(ab) + (5y-2)^2 = 0.$$

But $p_1 = -\dfrac{5}{y}$, $p_2 = 4$, $p_3 = 0$;

$$\therefore\; S_1 = \frac{5}{y},\quad S_2 = \frac{25-8y^2}{y^2},\quad S_3 = \frac{125-6y^4}{y^3},$$

$$\Sigma(ab) = 4,\quad \Sigma(a^2b) = \frac{20}{y},\quad \Sigma(a^2b^2) = 16.$$

Hence, substituting and reducing, we find for the final equation (as at p. 229)

$$y^4 + 12y^3 + 87y^2 - 200y + 100 = 0.$$

177. The following method of elimination, depending upon the expansion of an implicit algebraical function in descending powers of its variable, has the advantage of exhibiting as many terms as we please of the final equation.

The two equations $M(x, y) = 0$, $N(x, y) = 0$, between x and y, of the m^{th} and n^{th} degrees respectively, if in each we collect in successive groups the terms which are of the same dimensions, may be written, putting $\dfrac{y}{x} = u$,

$$x^m f(u) + x^{m-1} f_1(u) + \ldots = 0 \;\ldots\ldots\ldots\ldots\; (1),$$
$$x^n F(u) + x^{n-1} F_1(u) + \ldots = 0 \;\ldots\ldots\ldots\ldots\; (2),$$

where $f(u)$, $f_1(u)$, &c. are polynomials with determinate coefficients, of the degrees m, $m-1$, &c.; and $F(u)$, $F_1(u)$, &c. polynomials of the degrees n, $n-1$, &c. The m values of u

furnished by (1) are functions of x; and for $x = \infty$ they coincide with the m determinate roots of $f(\alpha) = 0$, which is an equation of the ordinary form

$$p_0\alpha^m + p_1\alpha^{m-1} + \&c. = 0,$$

and we will suppose it to be free from equal roots. We may therefore put $u = \alpha + e$, where e is a quantity that vanishes when $x = \infty$; then since $f(\alpha) = 0$, we get from (1) (Art. 27),

$$x^m \{ef'(\alpha) + \tfrac{1}{2}e^2 f''(\alpha) + \ldots\} + x^{m-1}\{f_1(\alpha) + ef_1'(\alpha) + \ldots\}$$
$$+ x^{m-2}\{f_2(\alpha) + \ldots\} = 0;$$

or, dividing by x^{m-1},

$$exf'(\alpha) + f_1(\alpha) + \frac{1}{x}\{\tfrac{1}{2}(ex)^2 f''(\alpha) + exf_1'(\alpha) + f_2(\alpha)\} + \ldots = 0.$$

Now let $x = \infty$, and let the limit of ex be denoted by α', then $\alpha' . f'(\alpha) + f_1(\alpha) = 0$, which will always give a finite value for α', as $f(\alpha) = 0$ has no equal roots. Since ex has for its limit the quantity just determined α', we may put $ex = \alpha' + e'$; then

$$u = \alpha + e = \alpha + \frac{\alpha'}{x} + \frac{e'}{x},$$

$$\text{and } y = \alpha x + \alpha' + e',$$

the series for y, when we restrict the development to the two first terms, e' being the remainder.

Next, substituting this value $\alpha + e$ for u in (2), we get

$$x^n\{F(\alpha) + eF'(\alpha) \ldots\} + x^{n-1}\{F_1(\alpha) + eF_1'(\alpha) + \ldots\} = 0,$$

or, since $ex = \alpha' + e'$, where e' vanishes when $x = \infty$,

$$x^n F(\alpha) + x^{n-1}\{\alpha' F'(\alpha) + F_1(\alpha)\} + x^{n-1}E = 0,$$

E denoting a quantity that vanishes when $x = \infty$; which is the development of $N(x, y) = 0$, restricted to its two first terms. If we now form a similar expression for every root $\alpha_1, \alpha_2 \ldots \alpha_m$ of $f(\alpha) = 0$, and multiply all these expressions

together, we shall obtain the final equation in x, which will be of the form

$$Ax^{mn} + A\Sigma\left\{\frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)}\right\} x^{mn-1} + Hx^{mn-1} = 0,$$

where A denotes the value of the symmetrical function of the roots of $f(\alpha) = 0$,

$$F(\alpha_1) . F(\alpha_2) \ldots F(\alpha_m);$$

and the symbol Σ extends to every one of those roots; α' being equal to $-\frac{f_1(\alpha)}{f'(\alpha)}$. Also H expresses the sum of a limited number of terms that vanish when $x = \infty$.

Hence we have a new proof of *Bezout's* theorem, the degree of the final equation being at most equal to mn; and we observe that the sum of the roots of the final equation in x, equals

$$-\Sigma\left\{\frac{\alpha' F'(\alpha) + F_1(\alpha)}{F(\alpha)}\right\}, \text{ where } \alpha' = -\frac{f_1(\alpha)}{f'(\alpha)}.$$

By proceeding in the same way, we may determine three terms of the development of u under the form

$$u = \alpha + \frac{\alpha'}{x} + \frac{\alpha''}{x^2} + \frac{e''}{x^2};$$

where α'' is given by the equation

$$\alpha''. f'(\alpha) + \tfrac{1}{2}\alpha'^2 f''(\alpha) + \alpha' f_1'(\alpha) + f_2(\alpha) = 0,$$

and $\frac{e''}{x^2}$ is the remainder of the series; and then three terms of the development of $N(x, y) = 0$; and next three terms of the final equation in x; and so on. The method is applicable to the elimination of $n-1$ unknown quantities from n equations; and it leads to the proof of *Bezout's* theorem in its most general statement.

178. As all the preceding methods suppose the equations to which they are applied to be rational, it is of importance

to be able to reduce an equation involving radicals, to a rational form. The extermination of radicals, considered generally, is only a case of elimination, as will appear from the following example.

Ex. 1. To reduce $x - \sqrt{x-1} + \sqrt[3]{x+1} = 0$ to a rational form.

Let $$y^2 = x - 1, \quad z^3 = x + 1;$$
$$\therefore\ x - y + z = 0;$$
this gives $y = x + z$, and therefore $y^2 = x - 1$ gives
$$z^2 + 2zx + x^2 - x + 1 = 0,$$
and it remains to eliminate z between this and
$$z^3 - x - 1 = 0.$$
Using the process of the greatest common measure, we find for the exact final equation,
$$x^6 - 3x^5 + 8x^4 + x^3 + 7x^2 - 7x + 2 = 0;$$
a result that may also be obtained directly from the proposed equation, by successive involutions.

Ex. 2. To form the equation which has a root
$$x = (c + \sqrt{c^2 - q^5})^{\frac{1}{5}} + (c - \sqrt{c^2 - q^5})^{\frac{1}{5}},$$
$$\text{or } x = a + b, \text{ suppose};$$
$$\therefore\ x^5 = a^5 + b^5 + 5ab\,(a^3 + b^3) + 10a^2b^2\,(a + b)$$
$$= a^5 + b^5 + 5ab\,(a + b)^3 - 5a^2b^2\,(a + b)$$
$$= 2c + 5qx^3 - 5q^2x;$$
$$\therefore\ x^5 - 5qx^3 + 5q^2x - 2c = 0.$$

Also, if we assume $a^m + b^m = 2c$, $a^m b^m = q^m$, then
$$a^m - b^m = 2\sqrt{c^2 - q^m}, \text{ and } a^m \text{ or } b^m = c \pm \sqrt{c^2 - q^m};$$
$$\therefore\ a + b = (c + \sqrt{c^2 - q^m})^{\frac{1}{m}} + (c - \sqrt{c^2 - q^m})^{\frac{1}{m}}$$
is (Art. 154, Ex. 3) a value of x in the equation
$$x^m - mqx^{m-2} + \frac{m\,(m-3)}{1\,.\,2}\,q^2x^{m-4} - \&c. = 2c.$$

SECTION X.

ON THE GENERAL SOLUTION OF EQUATIONS.

---

179. A REMARKABLE application of the theory of symmetrical functions is that made by *Lagrange* to the general solution of equations; by that means he solves the general equations of the first four degrees, by a uniform process, and one which includes all others that have been proposed for that purpose, the common relation of which to one another is thus made apparent.

It consists in employing an auxiliary equation, called a reducing equation, whose root is of the form

$$x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{n-1} x_n,$$

denoting by $x_1, x_2, \ldots x_n$ the n roots of the proposed equation, and by α one of the n^{th} roots of unity; and the principle on which it is based is as follows. Let y be the unknown quantity in the reducing equation, and let

$$y = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n,$$

$a_1, a_2, \ldots a_n$ denoting certain constant quantities; then if $n-1$ values of y, and suitable values of the constants $a_1, a_2, \ldots a_n$ can be found, so that we may have $n-1$ simple equations; those, together with the equation

$$-p_1 = x_1 + x_2 + \ldots + x_n,$$

will enable us to determine the n roots.

Now, supposing the constants in the value of y to preserve an invariable order a_1, a_2, &c., since the number of ways in which the n roots may be combined with them to form the

expression $a_1x_1 + a_2x_2 +$ &c. is the same as the number of permutations of n things taken all together; therefore the expression for y will have $n(n-1)\ldots 3.2.1$ values, and the equation for determining y will rise to the same number of dimensions, or will be of a degree higher than that of the proposed equation; hence the method will be of no use, unless such values can be assumed for the constants $a_1, a_2, \ldots a_n$ as shall make the solution of the equation in y depend upon that of an equation at most of $n-1$ dimensions. Now this may be done (at least when n does not exceed 4) by taking the n^{th} roots of unity $\alpha^0, \alpha, \alpha^2, \alpha^3, \ldots \alpha^{n-1}$ for $a_1, a_2, \ldots a_n$, so that

$$y = \alpha^0 x_1 + \alpha x_2 + \ldots + \alpha^{r-1}x_r + \alpha^r x_{r+1} + \ldots + \alpha^{n-1}x_n.$$

For, in the first place, with this assumption, the reducing equation will contain only powers of y which are multiples of n; for, since $\alpha^n = 1$,

$$\alpha^{n-r}y = \alpha^{n-r}x_1 + \alpha^{n-r+1}x_2 + \ldots + x_{r+1} + \alpha x_{r+2} + \ldots + \alpha^{n-r-1}x_n,$$

$$\text{or } \alpha^{n-r}y = \alpha^0 x_{r+1} + \alpha x_{r+2} + \ldots + \alpha^{n-1}x_r,$$

which is the same result as if we had interchanged x_1 and x_{r+1}. x_2 and x_{r+2}, &c., so that if y be a root of the reducing equation, $\alpha^{n-r}y$ is also a root; therefore the reducing equation, since it remains unaltered when $\alpha^{n-r}y$ is written for y, contains only powers of y which are multiples of n; if therefore we make $y^n = z$, we shall have a reducing equation in z of only $1.2.3\ldots(n-1)$ dimensions, whose roots will be the different values of z which result from the permutations of the $n-1$ roots $x_2, x_3, \ldots x_n$ among themselves. We shall now have, expanding and reducing,

$$z = y^n = u_0 + u_1\alpha + u_2\alpha^2 + \ldots + u_{n-1}\alpha^{n-1},$$

in which $u_0, u_1, u_2, \ldots u_{n-1}$ are determinate functions of the roots, which will be invariable for the simultaneous changes of x_1 into x_{r+1}, x_2 into x_{r+2}, &c., since $z = (\alpha^r y)^n$; and when their values are known in terms of the coefficients of the proposed equation, we shall immediately know the values of the roots. For let $z_0, z_1, z_2, \ldots z_{n-1}$ be the different values of z,

when 1, α, β, γ, ... λ, the roots of $y^n - 1 = 0$, are substituted for α; then since $y = \sqrt[n]{z}$, we have

$$x_1 + x_2 + \ldots + x_n = \sqrt[n]{z_0}$$
$$x_1 + \alpha x_2 + \ldots + \alpha^{n-1} x_n = \sqrt[n]{z_1}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots = \ldots$$
$$x_1 + \lambda x_2 + \ldots + \lambda^{n-1} x_n = \sqrt[n]{z_{n-1}};$$

therefore, adding, and taking account of the properties of the sums of the powers of 1, α, β, γ, &c. (Art. 154), we get

$$nx_1 = \sqrt[n]{z_0} + \sqrt[n]{z_1} + \ldots + \sqrt[n]{z_{n-1}}.$$

Again, multiplying the above system of equations respectively by 1, α^{n-1}, β^{n-1}, ... λ^{n-1}, we get

$$nx_2 = \sqrt[n]{z_0} + \alpha^{n-1}\sqrt[n]{z_1} + \beta^{n-1}\sqrt[n]{z_2} + \ldots + \lambda^{n-1}\sqrt[n]{z_{n-1}},$$

and so on for the rest. Hence, since $-p_1 = \sqrt[n]{z_0}$, and

$$\therefore\ (-p_1)^n = z_0 = u_0 + u_1 + \ldots + u_{n-1},$$

the problem is reduced to finding the values of u_1, u_2, ... u_{n-1}.

180. The reducing equation of $n-1$ dimensions, which has for its roots z_1, z_2, ... z_{n-1} the quantities by which the roots of the proposed equation have just been expressed, will require, for the determination of its coefficients, the solution of an equation of $1 . 2 . 3 \ldots (n-2)$ dimensions.

For if in the equation

$$z = (x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{n-1} x_n)^n,$$

we replace α by each of its powers α^2, α^3, ... α^{n-1}, and denote as before the corresponding values of z by z_2, z_3 ... z_{n-1}, and call the above value of z, z_1, we get

$$\begin{aligned} z_1 &= (x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4 + \ldots + \alpha^{n-1} x_n)^n \\ z_2 &= (x_1 + \ldots + \alpha^2 x_2 + \ldots\ldots\ldots\ldots)^n \\ z_3 &= (x_1 + \ldots\ldots + \alpha^3 x_2 + \ldots\ldots\ldots)^n \ldots (1) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ z_{n-1} &= (x_1 + \ldots\ldots\ldots\ldots\ldots + \alpha^{n-1} x_2)^n. \end{aligned}$$

In these expressions x_2 occupies, successively, the second, third, &c., n^{th} place; that is, all the places it can occupy subject to the condition that x_1 always stands first. If therefore in each of these expressions we make all possible permutations of x_3, x_4 ... x_n {the number of which is $1.2.3 \ldots (n-2)$} without altering the place of x_1 or x_2, we shall from each obtain $1.2.3 \ldots (n-2)$ values of z; and therefore on the whole we shall obtain the $1.2.3 \ldots (n-1)$ values which z admits of from the permutations of the $n-1$ roots $x_2, x_3, \ldots x_n$.

Now let

$$z^{n-1} + q_1 z^{n-2} + q_2 z^{n-3} + \ldots + q_{n-1} = 0, \ldots (2)$$

be the equation which has the above quantities z_1, z_2. and z_{n-1} for its roots; then the coefficients q_1, q_2, &c., will depend for their determination upon an equation whose degree is

$$1.2.3 \ldots (n-2).$$

For suppose that, by causing another root x_2 to stand first in the expressions (1), we form another system of values of $z_1, z_2, \ldots z_{n-1}$, and another equation of which they are the roots, similar to (2), viz.

$$z^{n-1} + q'_1 z^{n-2} + \ldots + q'_{n-1} = 0; \text{ and so on};$$

and let k be the number of such equations necessary to be formed in order to furnish all the values of z; then the first members of these equations multiplied together will be of the degree $k(n-1)$, and will be the final equation whose roots are all the values of z; and whose coefficients, being symmetrical functions of the roots of the proposed, are capable of being expressed rationally by its coefficients. Hence, as the degree of the final equation is equally expressed by $k(n-1)$ or $1.2.3 \ldots (n-1)$, we find $k = 1.2.3 \ldots (n-2)$. Also since there will be k equations similar to (2), there will be the same number of values of q_1; and the coefficients, consequently, of (2) will depend for their determination upon an equation whose degree is $1.2.3 \ldots (n-2)$.

To form the equation for determining q_1, we must divide the final equation in z by the first member of (2) which is one of its factors, and equate to zero the $n-1$ terms of the remainder; then $n-2$ of those equations will serve to determine q_2, q_3, &c., in terms of q_1; and substituting the values of q_2, q_3, &c., in the remaining equation, we shall have an equation in q_1 whose degree will be equal to $1 . 2 . 3 \ldots (n-2)$. If we know one system of values of the coefficients q_1, q_2, &c., and if we can solve the corresponding equation in z of $n-1$ dimensions, so as to obtain the values of z_1, z_2, &c., z_{n-1}, then the solution of the proposed equation follows, as has been shewn. The result of the entire process would be that the equation of $1.2.3 \ldots (n-1)$ dimensions, having for its roots all the values of z, would be resolved into $1 . 2 . 3 \ldots (n-2)$ factors of $n-1$ dimensions, by means of a single equation whose degree equals $1 . 2 . 3 \ldots (n-2)$.

181. When n is a composite number, the above general method admits of simplifications. For let n have a divisor m, so that $n = mp$ where m is not greater than p, and let α be a root of $y^m - 1 = 0$; then since $\alpha^m = 1$, $\alpha^{m+1} = \alpha$, $\alpha^{m+2} = \alpha^2$, &c., $\alpha^{2m} = 1$, $\alpha^{2m+1} = \alpha$, &c., we have

$$y = x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{n-1} x_n$$
$$= X_1 + \alpha X_2 + \alpha^2 X_3 + \ldots + \alpha^{m-1} X_m,$$

where $X_r = x_r + x_{m+r} + x_{2m+r} + \ldots + x_{n-m+r}$, and consists of p roots;

$$\therefore z = y^n = u_0 + u_1\alpha + u_2\alpha^2 + \ldots + u_{m-1}\alpha^{m-1},$$

where u_0, u_1, &c., are known functions of X_1, X_2, &c.; and when they are found in terms of the coefficients of the proposed equation, we shall be able to determine immediately the values of X_1, X_2, &c., as before. To deduce the value of the primitive roots x_1, x_2, x_3, ... x_n, we must regard separately those which compose each of the quantities X_1, X_2, &c., as the roots of an equation of p dimensions. Thus let the roots whose sum is X_1, be those of the equation

$$x^p - X_1 x^{p-1} + Lx^{p-2} - Mx^{p-3} + \ldots = 0 \ldots\ldots (1),$$

where L, M, &c., are unknown; then the first member of this equation is a divisor of the first member of the proposed, since all its roots belong to the latter. Hence, effecting the division and equating to zero the coefficients of x^{p-1}, x^{p-2}, &c., in the remainder, we shall have p equations in X_1, L, M, &c., of which the $p-1$ first will give the values of L, M, &c., in terms of X_1. It will then remain to solve the equation (1) so determined of p dimensions. Similarly, substituting the value of X_2 in place of that of X_1, we shall have an equation giving the next group of roots x_2, x_{m+2}, &c.; and so on.

182. In this case, that is when n is a composite number and $= mp$ where m is a prime number, the formation of the reducing equation will require the solution of an equation of only $\frac{1 \cdot 2 \cdot 3 \ldots n}{(m-1)\, m\, (1 \cdot 2 \cdot 3 \ldots p)^m}$ dimensions.

For since $y = X_1 + \alpha X_2 + \alpha^2 X_3 + \ldots + \alpha^{m-1} X_m$,

if every one of the roots found in X_1, X_2, &c., were affected with a different coefficient, since there are n of those roots, the number of distinct values, which y would be capable of acquiring from their permutations, would be $1 \cdot 2 \cdot 3 \ldots n$. But on account of the p roots in each group having the same coefficient. the number of values of y is diminished. Let μ be this number; then supposing all the roots in the group X_1 to have distinct coefficients and so to furnish $1 \cdot 2 \cdot 3 \ldots p$ permutations, the number of values of y would be increased to

$$1 \cdot 2 \cdot 3 \ldots p \times \mu;$$

next, if all the roots in X_2 received distinct coefficients, the number of values of y would become $(1 \cdot 2 \cdot 3 \ldots p)^2 \times \mu$; and so on; so that if every root in every group had a distinct coefficient, the number of values of y would be

$$(1 \cdot 2 \cdot 3 \ldots p)^m \times \mu,$$

which, as we have seen above, is equal to $1 \cdot 2 \cdot 3 \ldots n$. But, as shewn in Art. 179, the number of values of z, where

$$z = (X_1 + \alpha X_2 + \alpha^2 X_3 + \ldots + \alpha^{m-1} X_m)^m \ldots\ldots (1)$$

is $\frac{1}{m}$th of the number of values of y, and therefore is equal to $\mu \div m$. Also, if as before we denote by z_1 the value of z in equation (1), and by $z_2, z_3, \ldots z_{m-1}$ the values which z assumes when α is successively replaced by its powers $\alpha^2, \alpha^3, \ldots \alpha^{m-1}$, we may form an equation which has the quantities z_1, z_2, z_{m-1} for its roots, viz.

$$z^{m-1} + q_1 z^{m-2} + \&c. + q_{m-1} = 0\ ;\ \ldots\ldots\ (2)$$

and next by causing another of the quantities X_2 to stand first in the value of y, we may form another system of values of

$$z_1,\ z_2,\ \ldots\ z_{m-1},$$

and another equation similar to (2), viz.

$$z^{m-1} + q'_1 z^{m-2} + \ldots + q'_{m-1} = 0\ ; \text{ and so on.}$$

Let k denote the number of such equations necessary to be formed, in order to furnish all the values of z; then the first members of these equations multiplied together will be the final equation in z, and its degree will be $k(m-1)$, which is the same as the number of values of z, and equals $\mu \div m$. Therefore, substituting for μ its value, we find

$$k = \frac{1\,.\,2\,.\,3\,\ldots\,n}{m\,(m-1)\,(1\,.\,2\,.\,3\,\ldots\,p)^m}\,.$$

Since, therefore, there will be k equations similar to (2), there will be the same number of values of the coefficient q_1; and the coefficients, consequently, of (2) will depend for their determination upon an equation whose degree is equal to the value of k above written.

183. This is the point to which the investigation of the algebraical solution of equations was brought by Lagrange, and where it still remains at the present time. The method leads to the solution of equations of the 3rd and 4th degree, as we proceed to shew; but for the equation of the 5th degree

$$x^5 + px^4 + qx^3 + rx^2 + sx + t = 0,$$

if, taking α for an imaginary root of $x^5 - 1 = 0$, we assume

$$z = (x_1 + \alpha x_2 + \alpha^2 x_3 + \alpha^3 x_4 + \alpha^4 x_5)^5,$$

we may form the equation with determined coefficients whose roots are all the values of z, and whose degree will .

$$= 1 . 2 . 3 . 4 = 24:$$

and its first member will be capable of being resolved into 2×3 or six biquadratic equations of the form

$$z^4 + q_1 z^3 + q_2 z^2 + q_3 z + q_4 = 0;$$

where each of the coefficients q_1, q_2, &c., admits of 2×3 values, for different permutations of the roots; and will therefore depend upon the solution of an equation of the sixth degree. So that by this process the solution of an equation of the fifth degree will necessarily involve the solution of another equation of a higher degree than its own.

Ex. 1. $$x^3 - px^2 + qx - r = 0.$$

Let the roots be a, b, c, and let

$$y = a + \alpha b + \alpha^2 c;$$

$$\therefore\ z = y^3 = a^3 + b^3 + c^3 + 6abc + 3(a^2 b + b^2 c + c^2 a)\alpha$$
$$+ 3(a^2 c + b^2 a + c^2 b)\alpha^2,$$
$$= u_0 + u_1\alpha + u_2\alpha^2.$$

But u_1, u_2, are roots of the quadratic

$$u^2 - (u_1 + u_2)u + u_1 u_2 = 0,$$

and $u_1 + u_2 = 3\Sigma(a^2 b) = 3pq - 9r$ (Art. 159),

$$u_1 u_2 = 9\{abcS_3 + \Sigma(a^3 b^3) + 3a^2 b^2 c^2\}$$
$$= 9q^3 + 9(p^3 - 6pq)r + 81r^2.$$

Hence u_1, u_2 are known,

and $\therefore\ u_0 = p^3 - (u_1 + u_2)$, is known.

Hence, denoting by z_1, z_2, the values of z when α and α^2 are respectively written for α, we have

$$a + b + c = p,$$
$$a + \alpha b + \alpha^2 c = \sqrt[3]{z_1},$$
$$a + \alpha^2 b + \alpha c = \sqrt[3]{z_2};$$

from which we obtain the values of a, b, and c, viz.

$$a = \tfrac{1}{3}(p + \sqrt[3]{z_1} + \sqrt[3]{z_2}),$$

$$b = \tfrac{1}{3}(p + \alpha^2 \sqrt[3]{z_1} + \alpha \sqrt[3]{z_2}),$$

$$c = \tfrac{1}{3}(p + \alpha \sqrt[3]{z_1} + \alpha^2 \sqrt[3]{z_2}).$$

Ex. 2. $$x^4 - px^3 + qx^2 - rx + s = 0.$$

Since $4 = 2.2$, let α be a root of $y^2 - 1 = 0$, so that $\alpha^2 = 1$;

$$\text{then } y = x_1 + \alpha x_2 + x_3 + \alpha x_4 = X_1 + \alpha X_2,$$

$$\text{if } X_1 = x_1 + x_3, \qquad X_2 = x_2 + x_4;$$

$$\therefore z = y^2 = u_0 + \alpha u_1$$

where $u_0 = X_1^2 + X_2^2$, $u_1 = 2X_1X_2$, and $u_0 + u_1 = z_0 = p^2$.

Hence $u_1 = 2(x_1 + x_3)(x_2 + x_4)$, by interchanging the roots among themselves, will admit the two other values

$$2(x_1 + x_2)(x_3 + x_4), \text{ and } 2(x_1 + x_4)(x_2 + x_3),$$

and will therefore be a root of an equation of the form

$$u_1^3 - Mu_1^2 + Nu_1 - P = 0;$$

the coefficients being symmetrical functions of x_1, x_2, x_3, x_4, and consequently assignable in terms of p, q, r, s. It is easily seen that if we make $u_1 = 2q - 2u$, we shall have an equation in u whose roots are

$$x_1x_3 + x_2x_4, \; x_1x_2 + x_3x_4, \; x_1x_4 + x_2x_3;$$

and the transformed equation is (Art. 162)

$$u^3 - qu^2 + (pr - 4s)u - (p^2 - 4q)s - r^2 = 0.$$

Let u' be a root of this equation, then $u_1 = 2q - 2u'$; hence, making $\alpha = -1$,

$$z_1 = u_0 - u_1 = p^2 - 2u_1 = p^2 - 4q + 4u';$$

$$\therefore X_1 + X_2 = p, \; X_1 - X_2 = \sqrt{z_1};$$

$$\therefore X_1 = \tfrac{1}{2}(p + \sqrt{z_1}), \; X_2 = \tfrac{1}{2}(p - \sqrt{z_1}).$$

Hence x_1, x_3, may be regarded as roots of a quadratic

$$x^2 - X_1x + L = 0;$$

dividing the proposed by this, and putting the first term of the remainder equal to zero, we find

$$L = \frac{X_1^3 - pX_1^2 + qX_1 - r}{2X_1 - p};$$

therefore x_1, x_3, are known; and x_2, x_4, will result from the same formulæ by interchanging X_1 and X_2, or by changing the sign of the radical $\sqrt{z_1}$.

Ex. 3. $\frac{x^n - 1}{x - 1} = 0$, n being a prime number.

If r be one of the roots, and a be a primitive root of the prime number n, (that is, a number whose several powers from 1 to $n-1$, when divided by n, leave different remainders) it is proved (Art. 80) that all the roots of this equation may be represented by

$$r,\ r^a,\ r^{a^2},\ r^{a^3}, \dots r^{a^{n-2}}.$$

$$\text{Let } y = r + \alpha r^a + \alpha^2 r^{a^2} + \dots + \alpha^{n-2} r^{a^{n-2}},$$

α being a root of the equation $y^{n-1} - 1 = 0$. Therefore, observing that $\alpha^{n-1} = 1$, and $r^n = 1$,

$$z = y^{n-1} = u_0 + \alpha u_1 + \alpha^2 u_2 + \dots + \alpha^{n-2} u_{n-2} \dots\dots\dots (1),$$

u_0, u_1, &c. being rational and integral functions of r which do not change by the substitution of r^a, r^{a^2}, r^{a^3}, &c., in the place of r; for these quantities, regarded as functions of x_1, x_2, x_3, &c., do not alter by the simultaneous changes of x_1 into x_2, x_2 into x_3, &c., nor by the simultaneous changes of x_1 into x_3. x_2 into x_4, &c., to which correspond the changes of r into r^a, into r^{a^2}, &c.

Now every rational and integral function of r, in which $r^n = 1$, may be reduced to the form

$$A + Br + Cr^2 + Dr^3 + \dots + Nr^{n-1},$$

the coefficients $A, B, C, \dots N$ being given quantities independent of r; or, since in this case the powers

$$r,\ r^2,\ r^3, \dots r^{n-1},$$

may be represented, although in a different order, by

$$r,\ r^a,\ r^{a^2}, \ldots r^{a^{n-2}},$$

we may reduce every rational function of r to the form

$$A + Br + Cr^a + Dr^{a^2} + \ldots + Nr^{a^{n-2}}.$$

Therefore, if this function is such that it remains unaltered when r is changed into r^a, it follows that the new form

$$A + Br^a + Cr^{a^2} + Dr^{a^3} + \ldots + Nr$$

coincides with the preceding;

$$\therefore\ B = C,\ C = D,\ D = E,\ \&c.,\ N = B,$$

and therefore the function is reduced to the form

$$A + B\,(r + r^a + r^{a^2} + \ldots + r^{a^{n-2}}),\ \text{or}\ A - B,$$

since the sum of the roots $= -1$; hence each of the quantities u_0, u_1, u_2, &c., will be of the form $A - B$, and its value will be found by the actual development of $z = y^{n-1}$; so that we have the case where the values of u_0, u_1, u_2, &c., are known immediately, without depending upon the solution of any equation. Hence if we denote by 1, α, β, γ, &c., the $n-1$ roots of the equation $x^{n-1} - 1 = 0$, and by z_0, z_1, z_2, &c., the value of z answering to the substitution of these roots in the place of α in equation (1), we shall have, as in the former cases,

$$r = \frac{\sqrt[n-1]{z_0} + \sqrt[n-1]{z_1} + \sqrt[n-1]{z_2} + \ldots + \sqrt[n-1]{z_{n-1}}}{n-1},$$

an expression for one of the roots of the equation $x^n - 1 = 0$; and the other roots are r^2, r^3, &c.

Thus the solution of $x^n - 1 = 0$ is reduced to that of the inferior equation $y^{n-1} - 1 = 0$, of which 1, α, β, γ, &c. are the roots; also since $n-1$ is a composite number, the determination of α, β, γ, &c. will not require the solution of an equation of a higher degree than the greatest prime number in $n-1$; that is, the solution of $x^n - 1 = 0$ (n prime), may be

made to depend upon the solution of equations whose degrees do not exceed the greatest prime number which is a divisor of $n-1$.

Ex. 4. $$x^5-1=0.$$

The least primitive root of 5 is 2; for the powers of 2 from 1 to 4, when divided by 5, leave remainders 2, 4, 3, 1;

$$\therefore\ y = r + \alpha r^2 + \alpha^2 r^4 + \alpha^3 r^3;$$

$$\text{also } \alpha^4 = 1,\ r^5 = 1, \text{ and } r + r^2 + r^4 + r^3 = -1;$$

$$\therefore\ z = y^4 = -1 + 4\alpha + 14\alpha^2 - 16\alpha^3.$$

But the four roots of $y^4 - 1 = 0$, are

$$1,\ -1,\ \sqrt{-1},\ -\sqrt{-1};$$

$$\therefore\ z_0 = 1,\ z_1 = 25,\ z_2 = -15 + 20\sqrt{-1},$$

$$z_3 = -15 - 20\sqrt{-1};$$

$$\therefore\ x = \tfrac{1}{4}\left(-1 + \sqrt{5} + \sqrt[4]{-15 + 20\sqrt{-1}} + \sqrt[4]{-15 - 20\sqrt{-1}}\right).$$

ABEL'S EXTENSION OF LAGRANGE'S METHOD.

Some of the principal extensions of *Lagrange's* method made by later Mathematicians, are contained in the following Propositions relative to equations whose roots have the same property as those of $x^n - 1 = 0$, namely, that all the roots can be expressed rationally in terms of one of them.

184. If two roots of an irreducible equation are so connected that one of them can be expressed rationally in terms of the other, then *all* its roots will be capable of being represented either by one group or by several groups of quantities of the form $x\ \theta x\ \theta^2 x \ldots \theta^{n-1} x$, where θx denotes a rational function of x such that $\theta^n x = x$.

Let $f(x)=0$ be an irreducible equation of the μ^{th} degree, and let two of its roots x' and x_1 be connected by the equation $x'=\theta x_1$, where θx denotes a given rational function of x. Then since x' is a root of $f(x)=0$, we have $f(\theta x_1)=0$; therefore $f(\theta x)=0$ admits *one* of the roots x_1, and consequently it admits *all* the roots of $f(x)=0$; for, otherwise, $f(\theta x)$ and $f(x)$, which are both rational functions of x, would have a common divisor; and that is impossible since $f(x)=0$ is irreducible. Hence $f(\theta x)=0$ is satisfied by every one of the roots of $f(x)=0$; in other words, if x_r be a root of $f(x)=0$, then is θx_r likewise one of its roots. But θx_1 is a root of $f(x)=0$, therefore $\theta(\theta x_1)$ or $\theta^2 x_1$ is a root; hence also $\theta(\theta^2 x_1)$ or $\theta^3 x_1$ is a root, and so on; so that $f(x)=0$, has for roots all the terms of the series

$$x_1 \;\; \theta x_1 \;\; \theta^2 x_1 \;\; \theta^3 x_1 \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\; (1).$$

But as $f(x)=0$ cannot have more than μ different roots, some of these must recur; suppose therefore

$$\theta^{m+n}x_1=\theta^m x_1, \;\text{ or }\; \theta^n(\theta^m x_1)-\theta^m x_1=0;$$

this shews that the equation $\theta^n x - x=0$ has the root $\theta^m x_1$ in common with $f(x)=0$; it consequently admits all the roots of $f(x)=0$;

$$\text{therefore } \theta^n x_1 - x_1 = 0, \;\text{ or }\; \theta^n x_1 = x_1 \;\text{ and }\; \theta^{n+k}x_1=\theta^k x_1.$$

Hence the operation expressed by θ is such that, after being repeated a certain number n of times upon x, it reproduces x; and if the series (1) be continued beyond the n^{th} term, the same values will recur in the same order; so that in fact there will be only the n different values

$$x_1 \;\; \theta x_1 \;\; \theta^2 x_1 \ldots \theta^{n-1}x_1; \;\ldots\ldots\ldots\ldots\ldots\ldots\; (2)$$

and if $n=\mu$, which is necessarily the case for μ a prime number, these are all the roots of $f(x)=0$. This happens, as we have seen (Art. 76), for the equation $\dfrac{x^\mu-1}{x-1}=0$ when μ is a prime number.

But if μ be greater than n, let x_2 be another root of $f(x) = 0$ not comprised in group (2); then, as before, it may be shewn that all the terms of the series

$$x_2 \;\; \theta x_2 \;\; \theta^2 x_2 \ldots \theta^{n-1} x_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

are equally roots of $f(x) = 0$; and that it is only the n first that are different from one another; for since the equation

$$\theta^n x - x = 0$$

admits one of the roots x_1 of $f(x) = 0$, it admits all the other roots; and we have

$$\theta^n x_2 = x_2, \quad \theta^{n+k} x_2 = \theta^k x_2;$$

so that the terms of (3) are reproduced in the same order after the n^{th}. Also the roots

$$x_2 \;\; \theta x_2 \;\; \theta^2 x_2 \ldots \theta^{n-1} x_2; \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

are all distinct from one another, and from the roots (2).

For suppose $\theta^k x_2 = \theta^i x_2$, i and k being both less than n; then since the equation $\theta^k x - \theta^i x = 0$ admits the root x_2, it also admits the root x_1; therefore $\theta^k x_1 = \theta^i x_1$, which is impossible because the quantities (2) are all unequal. Neither can we have $\theta^k x_2 = \theta^i x_1$; for it would follow that

$$\theta^{n-k}(\theta^i x_1) = \theta^{n-k}(\theta^k x_2), \quad \text{or } \theta^{n-k+i} x_1 = \theta^n x_2 = x_2,$$

so that x_2 would belong to series (2), which is contrary to the supposition made relative to x_2.

Hence the number of different roots of $f(x) = 0$ contained in the groups (2) and (4) being $2n$, we must either have $\mu = 2n$ or $> 2n$. If $\mu > 2n$, then taking another root x_3 not comprised either in series (1) or (3), we may form another group of n distinct roots $x_3 \; \theta x_3 \; \theta^2 x_3 \ldots \theta^{n-1} x_3$, all different from the former; from whence it will follow that we must have either $\mu = 3n$ or $> 3n$. By continuing this process we shall produce all the roots; and as they appear only in groups each

consisting of n roots, the entire number of them will be mn, which must equal μ the degree of $f(x) = 0$. Hence we shall have all the roots distributed into a certain number m of groups each consisting of n terms, where $mn = \mu$; and the roots in every group will be liable to the same condition as the roots in the first group (2). When μ is prime so that $m = 1$, the roots can be all represented by a single group

$$x \;\; \theta x \;\; \theta^2 x \ldots \theta^{\mu-1} x, \text{ where } \theta^{\mu} x = x.$$

185. Let $x^n + p_1 x^{n-1} + \&c. + p_n = 0$ .... (5)
be the equation which has for its roots the group

$$x_1 \;\; \theta x_1 \;\; \theta^2 x_1 \ldots \theta^{n-1} x_1;$$

then for each of the m groups of roots there will be a similar equation; so that any one of the coefficients p_1 will admit of m values, and will depend for its determination upon an equation of the m^{th} degree,

$$y^m + q_1 y^{m-1} + \&c. + q_m = 0 \;\; \ldots\ldots\ldots\ldots\ldots\ldots \;\; (6).$$

Abel has shewn how to form these reducing equations; and he has proved that the coefficients p_1, p_2, &c. of (5) are all rational functions of the same root y_1 of (6); that the coefficients of the equation having for roots the next group

$$x_2 \;\; \theta x_2 \;\; \theta^2 x_2 \ldots \theta^{n-1} x_2,$$

are all rational functions of another root y_2 of (6); and so on; so that the solution of $f(x) = 0$ whose degree is a composite number, is thus reduced to the solution of equations of inferior degrees.

The reducing equation (6) cannot, of course, be solved algebraically, when m exceeds 4: but the equation (5), whose roots have the property that they can be represented by

$$x_1 \;\; \theta x_1 \;\; \theta^2 x_1 \ldots \theta^{n-1} x_1,$$

where θx denotes a rational function of x such that $\theta^n x = x$, and all similar equations belonging to the other groups, if we suppose their coefficients to be known, admit of algebraical solutions, as we shall shew in the next Article.

186. If the μ roots of any equation $f(x)=0$ can be represented by x, θx, $\theta^2 x$, ... $\theta^{\mu-1}x$, θx being a rational function of x such that $\theta^{\mu}x = x$, the equation may be solved algebraically.

According to *Lagrange's* assumption, let

$$\psi_n(x) = (x + \alpha^n.\theta x + \alpha^{2n}.\theta^2 x + \ldots + \alpha^{(\mu-1)n}.\theta^{\mu-1}x)^{\mu} \ldots (1),$$

α^n being a root of $x^{\mu}-1=0$. Then since $\theta^{\mu+\nu}x = \theta^{\nu}x$, if x be replaced by some other root $\theta^m x$, it will be found that

$$\psi_n(\theta^m x) = \psi_n(x).\alpha^{(\mu-m)n\mu};$$

so that the only change which $\sqrt[\mu]{\psi_n(x)}$ undergoes, when $\theta^m x$ is substituted in it for x, is to be multiplied by $\alpha^{(\mu-m)n}$; and by the same substitution $\psi_n(x)$ remains unaltered, and we have $\psi_n(x) = \psi_n(\theta^m x)$. Therefore, giving m all its values from 0 to $\mu-1$, and taking the sum of the results, we get

$$\mu\psi_n(x) = \psi_n(x) + \psi_n(\theta x) + \ldots + \psi_n(\theta^{\mu-1}x),$$

which shews (Art. 153) that $\psi_n(x)$ is a symmetrical function of all the roots of $f(x)=0$, and can therefore be expressed by the coefficients of $f(x)$ and θx, and may be considered as known and denoted by v_n. Hence, substituting this value for $\psi_n(x)$ in (1), taking the μ^{th} root of both sides, and then giving n all its values from 0 to $\mu-1$, we get

$$x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1}x = \sqrt[\mu]{v_0},$$

$$x + \alpha.\theta x + \alpha^2.\theta^2 x + \ldots + \alpha^{\mu-1}.\theta^{\mu-1}x = \sqrt[\mu]{v_1},$$

....

$$x + \alpha^{\mu-1}.\theta x + \alpha^{2(\mu-1)}.\theta^2 x + \ldots + \alpha^{(\mu-1)^2}.\theta^{\mu-1}x = \sqrt[\mu]{v_{\mu-1}}.$$

Therefore, adding together these equations, and taking account of the properties of the roots 1, α, α^2, &c., we get

$$\mu x = \sqrt[\mu]{v_0} + \sqrt[\mu]{v_1} + \sqrt{v_2} + \ldots + \sqrt[\mu]{v_{\mu-1}} \ldots\ldots\ldots\ldots (2),$$

where $\sqrt{v_0} = -p_1$, supposing $f(x) = x^{\mu} + p_1 x^{\mu-1} + \&c.$

This expression (2) for x may be transformed so as only to admit of μ values. For since by changing x into $\theta^m x$, $\sqrt[\mu]{v_n}$ is only altered by being multiplied by $\alpha^{(\mu-m)n}$, and consequently

$\sqrt[\mu]{v_1^{\mu-n}}$ by being multiplied by $\alpha^{(\mu-m)(\mu-n)}$, therefore $\sqrt[\mu]{v_n} \,.\, \sqrt[\mu]{v_1^{\mu-n}}$ remains unaltered since it is only multiplied by the factor $\alpha^{(\mu-m)\mu} = 1$. If therefore we assume

$$\sqrt[\mu]{v_n} \,.\, \sqrt[\mu]{v_1^{\mu-n}} = \phi_n(x), \text{ then } \phi_n(x) = \phi_n(\theta^m x);$$

from whence it follows, as in the case of $\psi_n(x)$, that $\phi_n(x)$ is a symmetrical function of all the roots of $f(x) = 0$, and may be considered as a known quantity and denoted by u_n;

$$\therefore \sqrt[\mu]{v_n} \,.\, \sqrt[\mu]{v_1^{\mu-n}} = u_n, \text{ or } \sqrt[\mu]{v_n} = \frac{u_n}{v_1} (\sqrt[\mu]{v_1})^n,$$

a formula which enables us to express each of the radicals in (2) by a power of $\sqrt[\mu]{v_1}$; and we thus get

$$\mu x = -p_1 + \sqrt[\mu]{v_1} + \frac{u_2}{v_1} (\sqrt[\mu]{v_1})^2 + \frac{u_3}{v_1} (\sqrt[\mu]{v_1})^3 + \ldots + \frac{u_{\mu-1}}{v_1} (\sqrt[\mu]{v_1})^{\mu-1},$$

a value of x expressed as a rational function of $\sqrt[\mu]{v_1}$, and consequently admitting of only μ values, which are the roots of the proposed equation. Hence it follows from Art. 184, that if two roots of an irreducible equation $f(x) = 0$ whose degree is a prime number, are connected by a rational equation $x' = \theta x_1$, then $f(x) = 0$ can be solved algebraically; and when the coefficients both of $f(x)$ and $\theta(x)$ are real quantities, the only operations requisite for that purpose are those detailed in the following proposition.

187. In order to solve an equation with real coefficients $f(x) = 0$, whose degree is a prime number μ, and whose roots can be represented by $x, \theta x, \theta^2 x, \ldots \theta^{\mu-1} x$, where θx denotes a rational function of x with real coefficients such that $\theta^\mu x = x$, it is requisite only to divide a right angle and another known angle each into μ equal parts, and to extract the square root of a single quantity.

Since it has been proved that

$$\psi_1(x) \text{ or } v_1 = (x + \alpha \,.\, \theta x + \alpha^2 \,.\, \theta^2 x + \ldots + \alpha^{\mu-1} \,.\, \theta^{\mu-1} x)^\mu$$

is a rational function of the coefficients of $f(x) = 0$, if those

coefficients be all real, and also those of θx, then v_1 will contain no imaginary quantities except those of the root α, which equals $\cos\frac{2\pi}{\mu}+\sqrt{-1}\sin\frac{2\pi}{\mu}$. Moreover $v_{\mu-1}$ is deduced from v_1 by changing α into its conjugate $\alpha^{\mu-1}$; hence v_1, $v_{\mu-1}$, are known imaginary quantities conjugate to one another, and we may consequently assume

$$v_1=\rho\,(\cos\omega+\sqrt{-1}\sin\omega),$$

$$v_{\mu-1}=\rho\,(\cos\omega-\sqrt{-1}\sin\omega).$$

But since $\sqrt[\mu]{v_n}\,.\,\sqrt[\mu]{v_1}^{\,\mu-n}=u_n$, making $n=\mu-1$, we get $\sqrt[\mu]{v_{\mu-1}}\,.\,\sqrt[\mu]{v_1}=u_{\mu-1}$. Now $u_{\mu-1}$ can be expressed rationally by the coefficients of $f(x)$ and θx, and contains therefore no other imaginary quantities except those found in α; and the value just obtained shews that $u_{\mu-1}$ does not change when α is replaced by its conjugate $\alpha^{\mu-1}$, therefore $u_{\mu-1}$ is a real quantity. Let a denote the numerical value of $u_{\mu-1}$, then since

$$\rho^2=(u_{\mu-1})^{\mu},\quad\therefore\ \sqrt[\mu]{\rho}=\sqrt{a}.$$

Hence $\sqrt[\mu]{v_1}=\sqrt{a}\left(\cos\dfrac{2k\pi+\omega}{\mu}+\sqrt{-1}\sin\dfrac{2k\pi+\omega}{\mu}\right)$,

where k is an integer, from which the value of any power $(\sqrt[\mu]{v_1})^n$ can be immediately obtained; also its coefficient $\frac{u_n}{v_1}$, since both u_n and v_1 are known quantities of the form $\beta+\gamma\sqrt{-1}$, may be represented by $f_n+g_n\sqrt{-1}$, where f_n, g_n are rational functions of the coefficients of $f(x)$ and θx, and of $\cos\frac{2\pi}{\mu}$ $\sin\frac{2\pi}{\mu}$, quantities introduced by the root α. Consequently the value of every root is given by the equation (the second member of which has $\mu-1$ terms)

$$\mu x+p_1=\sqrt{a}\left(\cos\frac{\omega+2k\pi}{\mu}+\sqrt{-1}\sin\frac{\omega+2k\pi}{\mu}\right)$$

$$+ (f_2+g_2\sqrt{-1})\, a \left\{\cos\frac{2(\omega+2k\pi)}{\mu} + \sqrt{-1}\sin\frac{2(\omega+2k\pi)}{\mu}\right\}$$

$$+ (f_3+g_3\sqrt{-1})(\sqrt{a})^3\left\{\cos\frac{3(\omega+2k\pi)}{\mu} + \sqrt{-1}\sin\frac{3(\omega+2k\pi)}{\mu}\right\} + \&c.,$$

and to get all the roots, k must be taken from 0 to $\mu-1$. This result shews, as was asserted, that the determination of the roots requires only the division of the angles π and ω into μ equal parts, and the extraction of the square root of a. The condition to which the roots are subject, namely, that they can be represented by x, θx, $\theta^2 x, \dots \theta^{\mu-1}x$, where θx denotes a rational function of x, shews that the roots of the proposed equation are either all real or all imaginary.

SECTION XI.

ON SOME PROPERTIES OF NUMBERS CONNECTED WITH THE THEORY OF EQUATIONS.

As introductory to the propositions which follow on the Theory of Numbers, we may consider the properties of the successive remainders when the terms of the arithmetical and geometrical progressions

$$a,\ 2a,\ 3a,\ \dots\ (p-1)\,a,$$

$$1,\ a,\ a^2,\ a^3,\ \dots\ a^{p-1},$$

are divided by p, a and p being two whole numbers.

188. If p be prime to a, and if we divide by p the $p-1$ successive multiples of a,

$$a,\ 2a,\ 3a,\ \&c.,\ (p-1)\,a,$$

the remainders of these divisions will be all different from one another.

For suppose that two multiples ma and $m'a$, both less than pa, give the same remainder r; then taking q and q' to express the integral quotients, we get

$$ma = pq + r,\quad m'a = pq' + r;$$

$$\therefore\ (m'-m)\,a = p\,(q'-q).$$

Hence as p is prime to a, it must divide $m'-m$, which is impossible since m and m' are both less than p; therefore no two remainders are alike.

Suppose therefore r, r', r'', &c. to be the $p-1$ different

remainders obtained by dividing a, $2a$, &c., $(p-1)a$ by p, and q, q', q'', &c. the corresponding integral quotients, then

$$a = pq + r,\ 2a = pq' + r',\ 3a = pq'' + r'', \text{ \&c.};$$

therefore, adding pa to both sides of each equation,

$$(p+1)a = (q+a)p + r,\ (p+2)a = (q'+a)p + r', \text{ \&c.}$$

Hence after having passed pa, which is the first term divisible by p, the following terms give the remainders already found in the same order; and it is evident that the same period of remainders will constantly recur after every term that is exactly divisible by p.

189. If, p and a being prime to one another, we divide by p the series of powers $1, a, a^2, a^3$, &c., there will be at least one of them before a^p, which will leave a remainder unity; and up to this least remainder, all the remainders will be different; and beyond it, the same remainders will recur in the same order.

As the remainders are all less than p, there cannot be more than $p-1$ which are different; therefore amongst the p first terms $1, a, a^2, a^3, \ldots a^{p-1}$ of the series, there must be at least two which give the same remainder. Let these be a^m, $a^{m'}$, and let their common remainder be r; then

$$a^m = pq + r,\ a^{m'} = pq' + r \ldots\ldots\ldots\ldots (1);$$

$$\therefore\ a^{m'} - a^m = (q'-q)p, \text{ or } a^m(a^{m'-m} - 1) = (q'-q)p;$$

and as p is prime to a, it must divide $a^{m'-m} - 1$.

Hence we get unity for a remainder, on dividing by p the power $a^{m'-m}$ which is less than a^p. But if p be not prime to a, the theorem is no longer true; for the equation $a^m = pq + r$ shews that any factors common to a and p must divide r, which cannot therefore be equal to unity; so that no term except the first can ever produce a remainder 1, when divided by p.

190. Next let a^n denote the least power, other than a^0, which, divided by p, leaves the remainder unity; then all

the preceding remainders will be unequal. For if for two powers a^m, $a^{m'}$, less than a^n, we could have the equations (1), we might thence conclude, as before, that the power $a^{m'-m}$ would leave a remainder 1; and consequently a^n would not be the least power that had that remainder. Now let

$$a^n = pq + 1,$$

then for the next succeeding powers we shall have

$$a^{n+1} = pqa + a, \quad a^{n+2} = pqa^2 + a^2, \text{ \&c.};$$

therefore for the period a^n, $a^{n+1} \dots a^{2n-1}$, the remainders will be successively the same as for the period a^0, a^1, a^2, ... a^{n-1}. For a^{2n} the remainder will be the same as for a^n, because the equation $a^n = pq + 1$ leads to $a^{2n} = pqa^n + a^n$; and in the same way it may be shewn that from a^{2n} to a^{3n-1}, and for all succeeding intervals, the same period of remainders constantly recurs.

191. Moreover we perceive from the equations

$$a^n = pq + 1, \quad a^{2n} = pqa^n + a^n, \quad a^{3n} = pqa^{2n} + a^{2n}, \text{ \&c.},$$

that the remainder unity belongs to all indices that are multiples of n; and that if any index greater than n gives a remainder unity, it must be a multiple of n; for if it were not so, then by continually subtracting n from it we should at last descend to a power, less than a^n, leaving a remainder 1; which is impossible, as a^n is the least power that has that remainder.

Hence we are furnished with an easy method of finding the remainder for any power of a, provided we know the remainders of the first period; and these are easily calculated, by observing that, in order to pass from the remainder of any term a^t to that of a^{t+1}, it is sufficient to multiply the remainder of a^t by a, and to divide the product by p.

Ex. 1. To find the remainder of 4^{898} when divided by 11.

Powers	4^0	4^1	4^2	4^3	4^4	4^5,
Remainders	1	4	5	9	3	1;

each remainder being formed by multiplying the preceding one by 4, and dividing by 11; thus the product 4×4 gives the remainder 5; the product 5×4 gives the remainder 9; and so on. We stop at 4^5 because it reproduces the remainder 1, and the first period of remainders has been obtained. Hence dividing 898 by 5, we find a remainder 3, which shews that 4^{898} leaves the same remainder as 4^3, viz. 9.

Ex. 2. The remainder of 3^{1000} divided by 13, is 3.

192. If p be a prime number, and a a number not divisible by p, then $a^{p-1} - 1$ is divisible by p.

Let q, q', q'', &c., r, r', r'', &c., be the quotients and remainders obtained by dividing by p the $p-1$ quantities

$$a, \ 2a, \ 3a, \ \&c., \ (p-1)\,a;$$

so that

$$a = pq + r, \quad 2a = pq' + r', \quad 3a = pq'' + r'', \ \&c.;$$

then multiplying all these equations together, and denoting by Q a whole number, we get

$$a \,.\, 2a \,.\, 3a \ldots (p-1)\,a = (pq+r)\,(pq'+r') \ldots$$
$$= p \,.\, Q + rr'r'' \ldots$$

The first member is $1 \,.\, 2 \,.\, 3 \ldots (p-1)\,a^{p-1}$; and as the $p-1$ remainders are all less than p, and all different, $rr'r''\ldots$ must coincide with $1 \,.\, 2 \,.\, 3 \ldots (p-1)$;

$$\therefore\ 1 \,.\, 2 \,.\, 3 \ldots (p-1)\,(a^{p-1} - 1) = p \,.\, Q.$$

Consequently, the first member is divisible by p; and if we suppose p to be a prime number, as it cannot divide

$$1 \,.\, 2 \,.\, 3 \ldots (p-1),$$

p must divide $a^{p-1} - 1$, a being any number not divisible by p; which is *Fermat's* Theorem.

193. When a^{p-1} is not the least power, other than a^0, which produces the remainder 1, we know from Art. 191 that the index of that least power will be a divisor of $p-1$. Thus

in the following series of powers of 5, with their remainders after being divided by 11,

$$5^0\ 5^1\ 5^2 \ldots\ldots\ldots 5^5 \ldots\ldots\ldots\ldots\ldots\ldots 5^{10},$$
$$1\ \ 5\ \ 3\ \ 4\ \ 9\ \ 1\ \ 5\ \ 3\ \ 4\ \ 9\ \ 1,$$

we see that the index of 5^5, the least power which has the remainder 1, is a divisor of $11 - 1$ or 10.

But whenever a^{p-1} is the least power, other than a^0, which gives the remainder 1, then p is a prime number. For from Art. 190 it appears that the remainders which precede the division of a^{p-1}, are all distinct; they must therefore coincide with the number $1, 2, 3, \ldots p-1$, but not in the natural order. Now if p admitted a prime factor r, then r would be one of those remainders, and we should have an equation such as $a^m = pq + r$, so that r would be also a factor of a; and consequently a and p would not be prime to one another; in which case, as we know, there would be no power of a, after a^0, that would give a remainder 1.

194. Suppose a and p not to be prime to one another; and let p be replaced by pp', where p is prime to a, and p' is the product of factors found in a; and let a^n be the lowest power of a that is divisible by p'; then the remainders obtained by dividing the first n terms of the series from a^0 to a^{n-1} by pp', will be all different, and will not recur.

For if possible, m being less than n, let

$$a^m = pp'.q + r, \quad a^{m+m'} = pp'.q' + r.$$
$$\therefore\ a^m(a^{m'} - 1) = pp'(q' - q).$$

Now $a^{m'} - 1$ cannot be divisible by p' since a and p' are not prime to one another (Art. 189); therefore a^m is divisible by p', which is impossible since $m < n$. Hence any remainder belonging to a power less than a^n, cannot recur. But if m be not less than n, the above equation is possible; and it shews that p, which is prime to a^m, divides $a^{m'} - 1$; so that

$$a^{m'} = pq + 1,$$
$$\text{and } a^{m'+n} = pqa^n + a^n.$$

But a^n is divisible by p', therefore pa^n is divisible by pp'; consequently $a^{n'+n}$ divided by pp' leaves the same remainder as a^n divided by pp'. Hence the terms beginning with a^n, when divided by pp', produce remainders that recur; and the n terms that precede a^n produce remainders that do not recur; n being the index of the lowest power of a that is divisible by the product of all the factors equal and unequal that a has in common with pp'.

195. If therefore p be a prime number, and a a number not divisible by p; on dividing by p the series

$$a^0, a^1, a^2, a^3 \dots a^n \dots a^{p-1},$$

it is either a^{p-1}, or a^n where n is a divisor of $p-1$, that first reproduces the remainder unity. In the former case, the remainders are all distinct and form a complete period of the numbers $1, 2, 3, \dots p-1$ in a certain order; in the latter case, the remainders are different from one another up to the division of a^n, and afterwards recur in the same order, forming only an imperfect period of some of the numbers $1, 2, 3 \dots p-1$. Thus if $p=11$ and $a=2$, we have a complete period of remainders

$$1 \quad 2 \quad 4 \quad 8 \quad 5 \quad 10 \quad 9 \quad 7 \quad 3 \quad 6$$

ending with the division of 2^9; because the division of 2^{10} by 11 reproduces the remainder 1, and the period of remainders comes over again. But if $a=4$, we have seen (Art. 191) that there is only an imperfect period of remainders 1, 4, 5, 9, 3. Any number less than p, whose powers from 0 to $p-2$, when divided by p, produce all the integers less than p for remainders, is called a primitive root of the prime number p. Hence for a number a to be a primitive root of a prime number p, it must be less than p, and such that a^{p-1} is the lowest power, other than a^0, which when divided by p leaves unity for a remainder. Every prime number p may be shewn to have as many primitive roots as there are numbers prime to $p-1$ in the series $1, 2, 3 \dots p$.

196. From the result of Art. 194, may be deduced some properties of recurring Decimals; for let $\frac{r}{p}$ be a proper fraction in its lowest terms, and let it be converted into a decimal in a scale of Notation whose radix is a, so that

$$\frac{r}{p} = 0, \; q_1 \, q_2 \, q_3 \cdots;$$

then q_1 is found by dividing ra by p leaving a remainder r_1, q_2 by dividing ra_1 by p leaving a remainder r_2, and so on; so that

$$r \; r_1 \; r_2, \; \&c.$$

are in fact the same as the remainders obtained by dividing by p the quantities

$$r \;\; ra \;\; ra^2 \;\; ra^3, \; \&c. \; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; (1).$$

Now, supposing p not to be prime to a, the division by p of the series of quantities (1), as we have seen, will produce first a set of n remainders that do not recur, and then a set that constantly recur: so that the recurring period of quotients will commence only at the $(n+1)^{\text{th}}$ figure from the decimal point, n being the lowest power of a that is divisible by all the factors equal and unequal that a has in common with p. If p be prime to a, the recurring period of quotients will commence immediately after the decimal point. Hence in the common scale of Notation, the recurring decimal which expresses $\frac{r}{p\,2^m 5^n}$, where p is prime both to r and 10, will have m or n places of figures before the recurring period, according as m or n is the greater.

197. If p be a prime number, $1 . 2 . 3 \ldots (p-1) + 1$ is divisible by p.

It appears by Art. 188 that, a being any number less than p, there is one and only one of the products

$$a.1 \quad a.2 \quad a.3 \ldots a(p-1)$$

which leaves a remainder 1 after being divided by p. If $a=1$ it is evidently the first term, and if $a=p-1$ it is the last

term that has this property. Therefore if we limit the values of a to the numbers 2, 3, ... $(p-2)$, then there is some one term of the series of products

$$(S_a) \quad a.2 \quad a.3, \text{ \&c. } \quad a.(p-2) \text{ .... } (1),$$

which when divided by p leaves 1 for remainder. Hence, if in S_a we substitute for a successively the numbers

$$2, 3, \ldots n, \ldots (p-2),$$

and call the resulting series of products S_2 S_3, &c., there will be in each, one term which when divided by p leaves a remainder 1. Let those terms be respectively represented by

$$2.\alpha \quad 3.\beta \ldots n.\delta \ldots (p-2)\,\lambda \text{ .... } (2),$$

where the factors that stand first are the values

$$2, 3, 4, \ldots (p-2)$$

that have been assigned to a, and the latter factors all belong to the same numbers 2, 3, &c. $(p-2)$, which are the latter factors in the series of products (1). Then the numbers

$$\alpha, \beta, \ldots \delta \ldots \lambda$$

are all different from one another; for if we would have $\delta = \alpha$, then we should have two terms 2α, $n\alpha$ in S_a leaving a remainder 1, after being divided by p, which is impossible. And we cannot have the factors of any term $n\delta$ equal to one another, for $n^2 - 1 = (n+1)(n-1)$ cannot be divisible by p unless $n = 1$, or $n = p - 1$, and both those values of a are excluded. Therefore the numbers $\alpha, \beta, \ldots \delta, \ldots \lambda$ must in a certain order coincide with 2, 3, 4, ... $(p-2)$. Also in the series (2) each product $n\delta$ must be repeated in the form δn, which is the term belonging to the series S_δ that leaves a remainder 1 after division by p. Therefore out of the series (2) there can be selected $\frac{1}{2}(p-3)$ terms whose product is

$$2 \,.\, 3 \,.\, 4 \ldots (p-2);$$

and as each of these terms is of the form $mp+1$, where m is an integer, their product will be of the same form; and we shall have

$$2 \,.\, 3 \,.\, 4 \ldots (p-2) = mp + 1;$$

therefore, multiplying by $p-1$, we get

$1.2.3...(p-1)=mp(p-1)+p-1$, or $1.2.3...(p-1)+1=m'p$, shewing that $1.2.3 ... (p-1)+1$ is divisible by p, which is *Wilson's* Theorem. The number p is exclusively a prime number; for if it had a divisor p', then p' would divide $1.2.3 ... (p-1)$; therefore p', and consequently p, could not divide $1.2.3 ... (p-1)+1$.

198. To find the highest power of any prime number p, which is contained in the product $1.2.3 ... n$.

Let m be the integral part of the quotient of n divided by p; then the product

$$p.2p.3p ... mp = 1.2.3 ... m.p^m,$$

contains all the factors of $1.2.3 ... n$ that are divisible by p. Next let m' be the integral part of the quotient of m divided by p; then $1.2.3...m'p^{m'}$ contains all the factors of $1.2.3...m$ that are divisible by p. In the same way, if m'' be the quotient of m' divided by p, $1.2.3...m''p^{m''}$ contains all the factors of $1.2.3 ... m'$ that are divisible by p; and so on, till we arrive at a quotient less than p; suppose this to be m''; then the index of the highest power of p contained in $1.2.3 ... n$, is $m+m'+m''$.

Ex. To find how often 7 is contained in $1.2.3 ... 1000$.

$$\text{Here } \frac{1000}{7}=142, \quad \frac{142}{7}=20, \quad \frac{20}{7}=2;$$

$$\therefore \; m+m'+m''=164.$$

199. Hence if m, n, p, q, &c. be whole numbers, and

$$m=n+p+q+\&c.$$

then the quotient of $1.2.3 ... m$ divided by

$$1.2.3 ... n \times 1.2.3 ... p \times 1.2.3 ... q \times \&c.$$

will be a whole number. For let t be any prime factor of the divisor, then

$$\frac{m}{t}=\frac{n}{t}+\frac{p}{t}+\frac{q}{t}+\&c.;$$

or, calling m', n', p', q', &c. the integral parts of the several quotients,

$$m' = \text{or} > n' + p' + q' + \&c.$$

Dividing again by t, and calling m'', n'', p'', q'', &c. the integral parts of the new quotients, we get

$$m'' = \text{or} > n'' + p'' + q'' + \&c.,$$

and so on, as long as the quotients are not all less than t. Therefore, by addition, we get

$$(m' + m'' + \&c.) = \text{or} >$$

$$(n' + n'' + \&c.) + (p' + p'' + \&c.) + (q' + q'' + \&c.) + \ldots;$$

but these different sums express the highest power of t contained in the several products of which the proposed expression is made up. As, therefore, there is no prime factor of its denominator which does not enter to at least an equal power in its numerator, the value of the proposed expression must be a whole number.

TRANSFORMATIONS OF CONGRUENCES ROOTS OF CONGRUENCES.

200. If $a - b = Mp$, a multiple of p, where p is a positive integer, and a and b integers positive or negative; a and b are said to be congruent, or equivalent, relative to p; and are called residuals one of the other relative to p, which is termed the modulus. Instead of writing

$$a = b + Mp,$$

the notation generally adopted is

$$a \equiv b, \text{ mod. } p.$$

Hence if r be the remainder after dividing a by p,

$$a \equiv r, \text{ mod. } p,$$

where r is comprised between 0 and p; or, if we do not confine ourselves to positive remainders, but take r to be the least number by which a must be either diminished or increased so as to become divisible by p, r will lie between $-\frac{1}{2}p$ and $\frac{1}{2}p$. Hence every number has a residual whose absolute

value is less than half the modulus, and is called its minimum residual; but if we consider only positive residuals, r lies between 0 and p.

201. The advantage of this notation is that it is analogous to that employed for equations; and most of the transformations which equations are capable of, may be applied to congruences. Thus if we have, relative to a modulus p, two congruences

$$a \equiv b, \quad a' \equiv b' \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1),$$

then, adding or subtracting, we shall have

$$a \pm a' \equiv b \pm b' \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2).$$

For the congruences (1) amount to

$$a = b + \text{a multiple of } p, \quad a' = b' + \text{a multiple of } p \ldots (3);$$

$$\therefore \; a \pm a' = b \pm b' + \text{a multiple of } p;$$

which is what (2) expresses.

Again, we may multiply a congruence by any whole number m; for if we have

$$a = b + \text{a multiple of } p, \text{ or } a \equiv b,$$

$$\text{then } ma = mb + \text{a multiple of } p, \text{ or } ma \equiv mb.$$

Also we may multiply together any number of congruences relative to the same modulus. For, multiplying together the equations (3), we get

$$aa' = bb' + \text{a multiple of } p, \text{ or } aa' \equiv bb',$$

the result of multiplying together the two congruences (1). Similarly, if we multiply by a third congruence relative to p, $a'' \equiv b''$, we get $aa'a'' \equiv bb'b''$; and so on, to n congruences; and if they all become identical with the first $a \equiv b$, we find $a^n \equiv b^n$: so that we may raise to any power the two members of the same congruence. Hence if

$$f(x) = p_0 x^n + p_1 x^{n-1} + \ldots + p_n$$

be a rational and integral function of x, with its coefficients whole numbers; and if we have, relative to a modulus p, $a \equiv b$, then we shall have the congruence $f(a) \equiv f(b)$ relative to the same modulus.

202. Also we may simplify a congruence by rejecting from both its members the same divisor, provided it be prime to the modulus. For if we have $ma \equiv mb$, then

$$ma = mb + \text{a multiple of } p = mb + m'p \text{ suppose};$$

and as m is prime to p, it must divide m'; and consequently we get

$$a = b + \text{a multiple of } p, \text{ or } a \equiv b.$$

Or, we may reject different divisors provided they be prime to the modulus and congruent relative to it. For suppose that we have $ma \equiv nb$, and that the divisors m and n are both prime to the modulus p, and such that $m \equiv n$; then we shall have $a \equiv b$; for if not, let $a \equiv b + r$ where r is less than p;

$$\therefore\ ma \equiv nb + nr,$$

$$\text{or, since } ma \equiv nb, \quad nr \equiv 0;$$

but n is prime to p, and r is less than p, therefore we must have $r = 0$, or $a \equiv b$. Hence we cannot from $a^n \equiv b^n$, mod. p, infer $a \equiv b$, mod. p. Thus $7^2 \equiv 3^2$, mod. 5, does not lead to $7 \equiv 3$, mod. 5; but $7^2 \equiv 3^2$, mod. 4, leads to $7 \equiv 3$, mod. 4.

203. If a be any number not divisible by the prime number p, then $a^{p-1} - 1$ is divisible by p; in other terms

$$a^{p-1} \equiv 1, \text{ mod. } p.$$

If we form the $p-1$ multiples of a,

$$a,\ 2a,\ 3a,\ \ldots\ (p-1)\,a \ \ldots\ldots\ldots\ (1),$$

we see that not one of them is divisible by p; and that every one of them, when divided by p, leaves a different remainder; for if two of them ma, na, left the same remainder, then their difference $(m-n)\,a$ would be divisible by p, which is impossible because $m-n$ is less than p. Those remainders must therefore be, in a certain order, the numbers

$$1,\ 2,\ 3,\ \ldots\ (p-1)\ \ldots\ldots\ldots\ (2).$$

Hence the numbers (1) being congruent with the numbers (2), we might form with them $p-1$ congruences of the form

$ma \equiv \mu$, where ma is one of the products (1), and μ one of the remainders (2). Then multiplying all these congruences together, we should find

$$1 \cdot 2 \cdot 3 \ldots (p-1)\, a^{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots (p-1);$$

and as the common factor of this congruence is prime to p the modulus, we may suppress it, and we get

$$a^{p-1} \equiv 1, \text{ mod. } p.$$

This proof of *Fermat's* Theorem, it will be perceived, does not in reality differ from that at Art. 192; but it shews the advantages, in point of brevity and clearness, of the Notation for Congruences, for conducting researches of this sort.

204. If p be a prime number, then $1 \cdot 2 \cdot 3 \ldots (p-1)+1$ is divisible by p; or in other terms

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv -1, \text{ mod. } p.$$

Let a be one of the numbers $1, 2, 3, \ldots (p-1)$, and let the $p-1$ products be formed

$$a, 2a, 3a, \ldots (p-1)\, a.$$

In this series there is some one term ma that, when divided by p, leaves a remainder 1; and its factors must be unequal unless $a=1$ or $p-1$, for $a^2-1=(a+1)(a-1)$ cannot be divisible by p, as a is less than p, unless either $a=1$ or $a=p-1$; consequently the numbers $2, 3, 4, \ldots (p-2)$ may be grouped in pairs, so that the product of each pair is congruent with unity; and multiplying together all the congruences thus obtained, we find

$$2 \cdot 3 \cdot 4 \ldots (p-2) \equiv 1;$$

therefore multiplying this by $p-1$,

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv p-1, \text{ or } 1 \cdot 2 \cdot 3 \ldots (p-1)+1 \equiv 0;$$

which is *Wilson's* Theorem. As was observed at Art. 197 this property belongs exclusively to prime numbers. For if p be a composite number, and p' one of its divisors, and therefore less than p; then p' will divide $1 \cdot 2 \cdot 3 \ldots (p-1)$ and cannot therefore divide the same product augmented by

unity; and of course p cannot divide a number which one of its factors does not divide.

205. If by $f(x)$ we denote as usual a polynomial of the form $p_0x^n + p_1x^{n-1} + \ldots + p_n$ whose coefficients are whole numbers; and if when x receives any integral value a or $-a$, $f(x)$ becomes divisible by the positive integer p, then $f(x)$ for that value of x is said to be congruent with zero relative to p: so that, as has been stated, the equation

$$f(x) = \text{a multiple of } p$$

is called a congruence, and is generally expressed by

$$f(x) \equiv 0, \text{ mod. } p,$$

and a is called a root of it.

The Theory of Numbers solves several of the same Problems relative to congruences, that the Theory of Equations solves relative to equations: and in particular proposes to find the values of x which satisfy the congruence

$$f(x) \equiv 0, \text{ mod. } p.$$

206. If this congruence is satisfied by $x = a$, it will also be satisfied by $x = a + mp$, m being any integer; for $f(x)$ by this substitution will evidently become $f(a)$ + a multiple of p. Hence every solution of $f(x) \equiv 0$, furnishes an infinite number of other solutions, which however are all equivalent relative to the modulus p. The different solutions contained in the formula $x = a + mp$ may be deduced from any one of them; and such a value may always be assigned to the integer m, that every value of $a + mp$ may be comprised between the limits $-\frac{1}{2}p$, and $\frac{1}{2}p$, or between 0 and p. It is only necessary therefore to consider the solutions contained within these limits; so that the roots of the congruence $f(x) \equiv 0$, mod. p, may be restricted to mean the values of x between 0 and p, which render $f(x)$ divisible by p. A congruence $f(x) \equiv 0$ is identical when all its coefficients are divisible by the modulus; and it is impossible, if all its coefficients are divisible by the

modulus except the term which is independent of x; for no integral value of x can make $pf_1(x)+p_n$ divisible by p, if p_n be not divisible by p.

207. If $F(x)$ denote another rational polynomial with integral coefficients, we may for the congruence

$$f(x) \equiv 0, \text{ mod. } p$$

substitute the equivalent congruence,

$$f(x) + pF(x) \equiv 0,$$

and dispose of the indeterminate coefficients of $F(x)$ so as to reduce below p, or below $\frac{1}{2}p$, all the coefficients of the congruence. When the modulus is a prime number, we may always transform a congruence so that the coefficient of its first term shall be unity.

Let $p_0x^n + p_1x^{n-1} + \ldots + p_n \equiv 0$ be a congruence whose modulus p is a prime number, and whose coefficients are all comprised between 0 and p, or between $-\frac{1}{2}p$ and $\frac{1}{2}p$: then if we add to its first member another polynomial

$$p\,(q_1x^{n-1} + q_2x^{n-2} + \ldots + q_n), \text{ we get}$$

$$p_0\,(x^n + \frac{p_1+pq_1}{p_0}\,x^{n-1} + \&c.) \equiv 0, \text{ mod. } p;$$

now p_0 being less than p is prime to p; and we may determine q_1, q_2, &c., so that $\frac{p_1+pq_1}{p_0}$, &c., may be whole numbers t_1, t_2, &c., comprised between 0 and p; or between $-\frac{1}{2}p$ and $\frac{1}{2}p$. The congruence will then become

$$p_0\,(x^n + t_1x^{n-1} + \ldots + t_n) \equiv 0, \text{ mod. } p,$$

or, since p_0 is prime to the modulus,

$$x^n + t_1x^{n-1} + \ldots + t_n \equiv 0,$$

where the coefficient of the first term is unity.

Thus the congruence $(2x-1)(3x-2) \equiv 0$, mod. 7, which has 3 and 4 for roots, may be reduced to

$$3x^2 + 1 \equiv 0, \text{ or } x^2 - 2 \equiv 0,$$

by adding or subtracting multiples of 7.

208. **A congruence relative to a prime modulus, and which is not identical, has at most as many roots as there are units in its degree.**

Let a congruence of the n^{th} degree, and having unity for the coefficient of its first term, be

$$f(x) \equiv 0, \text{ mod. } p, \ldots\ldots\ldots (1),$$

and let a be a root; then dividing $f(x)$ by $x-a$, we get

$$f(x) = (x-a) f_1(x) + f(a),$$

and since $f(a)$ is divisible by p, the congruence is reduced to

$$(x-a) f_1(x) \equiv 0, \text{ mod. } p.$$

Now let b be a second root, then

$$(b-a) f_1(b) \equiv 0, \text{ mod. } p;$$

but $b-a$ is less than p, and therefore prime to it,

$$\therefore f_1(b) \equiv 0, \text{ mod. } p,$$

so that b is a root of $f_1(x) \equiv 0$ (2), the coefficient of its first term being unity. Hence it results that the congruence (1) whose degree is n, can have only one root more than the congruence (2) whose degree is $n-1$. Similarly, the latter can have only one root more than $f_2(x) \equiv 0$ (3), whose degree is $n-2$, and the coefficient of its first term unity. Consequently the proposed congruence can have only two roots more than (3); and in the same way it may be shewn that the proposed can have only $n-1$ roots more than the congruence of the first degree, $x-l \equiv 0$, which admits but the single root l. Therefore a congruence of the n^{th} degree, relative to a prime modulus, cannot have more than n roots; but it may have fewer or none at all.

209. Suppose that $f(x) \equiv 0$, a congruence of the n^{th} degree and with unity for the coefficient of its first term, has actually n roots $a, b, c, \ldots l$; then these n roots will also belong to the congruence

$$f(x) - (x-a)(x-b) \ldots (x-l) \equiv 0;$$

but this is only of the $(n-1)^{\text{th}}$ degree; it is therefore identical, and consequently we have (Art. 206)

$$f(x) = (x-a)(x-b) \dots (x-l) + p.F(x),$$

where $F(x)$ denotes a rational and integral function of x with its coefficients whole numbers.

210. By *Fermat's* Theorem, the congruence

$$x^{p-1} - 1 \equiv 0, \text{ mod. } p,$$

admits of the $p-1$ roots 1, 2, 3, &c. $(p-1)$; if therefore $f(x)$ be a divisor of $x^{p-1}-1$, or more generally of $x^{p-1}-1$ increased by a polynomial of the degree $p-1$ such as $pF(x)$, then the congruence $f(x) \equiv 0$ will have as many roots as it has dimensions. For let

$$x^{p-1} - 1 + p \,.\, F(x) = f(x) \,.\, f_1(x);$$

then the congruence of the degree $p-1$,

$$f(x) \,.\, f_1(x) \equiv 0,$$

admits the roots 1, 2, 3, &c. $(p-1)$; but these roots also belong to the following congruences

$$f(x) \equiv 0, \;\; f_1(x) \equiv 0,$$

and therefore each of them has as many roots as it has dimensions; for if one of them had fewer roots than the units in its degree, the other would have more, which is impossible.

211. We are hence conducted to a simple process for determining the roots of a congruence relative to a prime modulus. First we observe that if q denote the quotient of the division of $f(x)$ by $f_1(x)$, and $f_2(x)$ be the remainder, we have

$$f(x) = q \,.\, f_1(x) + f_2(x);$$

which shews that if any value of x make $f_1(x)$ along with either $f(x)$ or $f_2(x)$, divisible by p, it must make the third function also divisible by p. Consequently the roots common to two congruences $f(x) \equiv 0$, $f_1(x) \equiv 0$, must also belong to $\phi(x) \equiv 0$, where $\phi(x)$ denotes the greatest common divisor

of $f(x)$ and $f_1(x)$; regard being had to the way in which $\phi(x)$ is found. Now if $f(x) \equiv 0$ be any proposed congruence relative to a prime modulus p, it can only have for roots whole numbers less than p, which all belong to the congruence $x^{p-1} - 1 \equiv 0$ relative to the same modulus. Therefore we have only to find the roots common to the two congruences $f(x) \equiv 0$, $x^{p-1} - 1 \equiv 0$; and these belong to $\phi(x) \equiv 0$, where $\phi(x)$ is the greatest common divisor of their first members. If $\phi(x)$ does not exist, the proposed congruence has no root; if $\phi(x)$ exists and is of the m^{th} degree, the proposed has m roots which are those of $\phi(x) \equiv 0$; roots that necessarily exist, because $\phi(x)$ is a divisor of $x^{p-1} - 1$. In finding this greatest common divisor, we may pursue the ordinary method; except that we may neglect all the terms that have p for a factor; and in order that all the divisions may be effected without introducing fractional coefficients, we may add to the coefficient of the first term of each dividend such a multiple of p as to make it divisible by the first term of the corresponding divisor.

Ex. To find the roots of the congruence

$$x^5 - 3x^4 - 2x^3 - 2x^2 + x - 2 \equiv 0, \text{ mod. } 7.$$

Dividing $x^6 - 1$ by the first member and neglecting multiples of 7, we find for the first remainder

$$-3x^4 + x^3 - 2x^2 - x - 2.$$

Next dividing the first member of the congruence by this remainder, we find $2x^3 - x^2 - 2x + 1$ for the second remainder; in which operation the terms $-7x^5$ and $-7x^4$ have been successively added to the dividend to avoid fractional coefficients. Finally, dividing the first remainder by the second and neglecting, as before, multiples of 7, we find the third remainder equal to zero; it having been necessary to add the term $-7x^4$ to the dividend before effecting the division. Hence the proposed congruence has three roots belonging to the congruence of the third degree

$$2x^3 - x^2 - 2x + 1 \equiv 0, \text{ mod. } 7;$$

or, adding $7x^2 - 7$ to the first member and dividing by 2,

$$x^3 + 3x^2 - x - 3, \text{ or } (x-1)(x+1)(x+3) \equiv 0.$$

Consequently the proposed congruence admits the three roots $1, -1, -3$; which may be replaced by 1, 6, 4.

212. If the modulus p be a prime number, the congruence

$$(x-1)(x-2)(x-3)\ldots(x-p+1) - x^{p-1} + 1 \equiv 0, \text{ mod. } p,$$

admits of the $p-1$ roots $1, 2, 3, \ldots p-1$; and as its degree is only $p-2$ when its first member is arranged according to powers of x, all its coefficients must be divisible by p. If therefore we denote by s_1, s_2, &c. the sum of the numbers $1, 2, 3, \ldots p-1$; the sum of the products of every two; &c., and by s_{p-1} the product of all of them, we have

$$s_1 \equiv 0, \; s_2 \equiv 0, \; \&c. \; s_{p-1} + 1 \equiv 0,$$

relative to the modulus p. The last of these congruences is *Wilson's* theorem. Moreover the coefficients of the equation

$$(x-1)(x-2)(x-3)\ldots(x-p+1) = 0,$$

when arranged according to powers of x, being, with the exception of the last term, multiples of p, *Newton's* formulæ for the sums of the powers of the roots of an equation (Art. 151) shew that the sum of the m^{th} powers of the $p-1$ roots $1, 2, 3, \ldots (p-1)$ is always divisible by p, unless m be a multiple of $p-1$.

BINOMIAL CONGRUENCES, PRIMITIVE ROOTS.

The properties of Binomial Congruences are analogous to those of Binomial Equations; and throughout the following investigation of them we suppose the modulus p to be a prime number.

213. The roots common to the two congruences

$$x^m \equiv 1, \quad x^n \equiv 1 \,\ldots\ldots\ldots\, (1),$$

also belong to $x^t \equiv 1$, where t is the greatest common measure of m and n; this follows from Art. 211, because $x^t - 1$ is the

greatest common divisor of $x^m - 1$ and $x^n - 1$; and conversely, every root of the congruence $x^t \equiv 1$, satisfies the two congruences (1).

Hence the roots of any proposed congruence, $x^m \equiv 1$, since they are integers between 0 and p, all satisfy $x^{p-1} \equiv 1$ by *Fermat's* theorem; and, consequently, are also roots of $x^t \equiv 1$, t being the greatest common measure of m and $p-1$. As $x^t - 1$ is a divisor of $x^{p-1} - 1$, $x^t \equiv 1$ has exactly t roots (Art. 210), the same number of roots as the proposed has: if m is prime to $p-1$, then $t = 1$, and the congruence $x^m \equiv 1$ has no root besides unity. Hence we may limit our investigation of the roots of the congruence

$$x^m \equiv 1, \text{ mod. } p$$

to the case where m is a divisor of $p-1$.

214. If α be a root of $x^m \equiv 1$, mod. p, where m is a divisor of $p-1$, then α^n, any power of α, or the minimum residual of α^n, is also a root.

For if we have $\alpha^m \equiv 1$, then $\alpha^{mn} \equiv 1$, or $(\alpha^n)^m \equiv 1$; and if β denote the minimum residual of α^n, then $\alpha^n \equiv \beta$, $\therefore \beta^m \equiv 1$. Consequently all the terms of the series α, α^2, α^3, &c., as well as the minimum residuals of those quantities, are roots of $x^m \equiv 1$. But since $\alpha^m \equiv 1$, we have also $\alpha^{m+1} \equiv \alpha$, $\alpha^{m+2} \equiv \alpha^2$, &c.; so that the series of powers of α contains at most m terms having different residuals; and these residuals recur in periods of m terms. If no two of the first m terms α, α^2, $\alpha^3 \ldots \alpha^m$ are equivalent, that is, congruent relative to the modulus p, then their residuals are the m roots of the proposed congruence. In the contrary case, if we have two terms whose indices are less than m congruent with one another, $\alpha^{n+n'} \equiv \alpha^{n'}$; then, α being prime to p, we get by dividing by $\alpha^{n'}$, $\alpha^n \equiv 1$, and consequently α is a root of the congruence $x^n \equiv 1$, of a degree inferior to m.

It hence results that if α be a root of the congruence $x^m \equiv 1$, not belonging to any congruence $x^n \equiv 1$ where $n < m$,

then the m roots of the proposed will be the residuals of the m powers of a, a, a^2, a^3, ... a^m. The primitive roots of the congruence $x^m \equiv 1$, where m is a divisor of $p-1$, are those which do not belong to any congruence $x^n \equiv 1$, where $n < m$. Any primitive root by its different powers can produce all the other roots. Any non-primitive root of $x^m \equiv 1$, belonging to $x^n \equiv 1$ where $n < m$ but is not a divisor of m, belongs also to a third congruence $x^{n'} \equiv 1$ where n' is a divisor of m.

Ex. $x^6 \equiv 1$, mod. 7; here $x = 3$; and the powers of 3, 1, 3; 3^2, 3^3, 3^4, 3^5 or their residuals 1, 3, 2, 6, 4, 5, are the six roots. Also the numbers 1, 2, 2^2, 2^3, 2^4, 2^5 are roots; but as their residuals are 1, 2, 4, 1, 2, 4, they only furnish three different roots. Hence 3 is a primitive root of the congruence $x^6 \equiv 1$, and 2 a non-primitive root; and we perceive that 2 is a root of $x^3 \equiv 1$," mod. 7, a congruence whose degree is a divisor of 6.

215. In the congruence $x^m \equiv 1$, let $m = q^\mu$; then every non-primitive root of $x^{q^\mu} \equiv 1$, (2) belongs to $x^t \equiv 1$ where t is a divisor of q^μ and also of $q^{\mu-1}$; consequently the root belongs to $x^{q^{\mu-1}} \equiv 1$, (3). Moreover all the roots of (3) are roots of (2), and their number is $q^{\mu-1}$; consequently the number of primitive roots of the proposed is $q^\mu - q^{\mu-1}$.

Suppose now that $m = q^\mu r^\nu \dots s^\sigma$, q, r, ... s being its unequal prime factors. Let α, β, ... λ be primitive roots respectively, of

$$x^{q^\mu} \equiv 1,\ x^{r^\nu} \equiv 1,\ \&c.,\ x^{s^\sigma} \equiv 1;$$

then will $\alpha\beta \dots \lambda$ be a primitive root of the proposed congruence, $x^m \equiv 1$. First of all, it is evident that $\alpha\beta \dots \lambda$, or its residual, is a root: for having

$$\alpha^q \equiv 1,\ \beta^{r^\nu} \equiv 1,\ \&c.,\ \lambda^{s^\sigma} \equiv 1,\ \text{we have}$$
$$(\alpha\beta \dots \lambda)^{q^\mu r^\nu \dots s^\sigma} \equiv 1.$$

Now if the product $\alpha\beta \dots \lambda$ be not a primitive root of the proposed, it will be a root of $x^t \equiv 1$ whose degree t is a

divisor of m; and there will be at least one of the prime factors of m, a less power of which will be found in t than in m. Let this be q, then t will divide $q^{\mu-1}r^{\nu}\ldots s^{\sigma}$, and consequently $\alpha\beta\ldots\lambda$ will be a root of the congruence

$$x^{q^{\mu-1}r^{\nu}\ldots s^{\sigma}} \equiv 1 \text{; we shall therefore have}$$

$$(\alpha\beta\ldots\lambda)^{q^{\mu-1}r^{\nu}\ldots s^{\sigma}} \equiv 1 \text{; but we have also}$$

$$(\beta\gamma\ldots\lambda)^{q^{\mu-1}r^{\nu}\ldots s^{\sigma}} \equiv 1 \text{; therefore by division we get}$$

$$\alpha^{q^{\mu-1}r^{\nu}\ldots s^{\sigma}} \equiv 1;$$

from which we see that α is a root of the two congruences

$$x^{q^{\mu-1}r^{\nu}\ldots s^{\sigma}} \equiv 1, \text{ and } x^{q^{\mu}} \equiv 1;$$

and consequently of $x^{q^{\mu-1}} \equiv 1$, since $q^{\mu-1}$ is the greatest common divisor of the degrees of the two preceding congruences. Therefore α is not, as was supposed, a primitive root of $x^{q^{\mu}} \equiv 1$. Consequently $\alpha\beta\ldots\lambda$, or its residual, is a primitive root of the proposed congruence.

216. By reasonings similar to those employed at Art. 79 it may be shewn that all the roots, both primitive and non-primitive, of $x^{m} \equiv 1$, where $m = q^{\mu}r^{\nu}\ldots s^{\sigma}$, are comprised in the formula $x = \alpha\beta\ldots\lambda$, which is composed of the product of one root α belonging to $x^{q^{\mu}} \equiv 1$, one root β belonging to $x^{r^{\nu}} \equiv 1$, &c., and one root λ belonging to $x^{s^{\sigma}} \equiv 1$. And the same formula furnishes the primitive roots of the proposed congruence, if we take for α. β, ... λ the different primitive roots of the congruences to which those roots respectively belong. And as the number of primitive roots α is $q^{\mu}\left(1-\frac{1}{q}\right)$, the number of primitive roots β is $r^{\nu}\left(1-\frac{1}{r}\right)$, &c., and that of the primitive roots λ is $s^{\sigma}\left(1-\frac{1}{s}\right)$; therefore the number of primitive roots of the proposed congruence, $x^{m} \equiv 1$, is

$$m\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots\left(1-\frac{1}{s}\right);$$

a formula which also expresses how many numbers there are prime to m and less than m.

Ex. $x^6 \equiv 1$, mod. 13. The roots will be found to be

$$10 \quad 4 \quad 3 \quad 9 \quad 12 \quad 1;$$

and the congruences of inferior degrees with their roots, are

$$x^4 \equiv 1, \quad 5 \quad 8 \quad 12 \quad 1$$

$$x^3 \equiv 1, \quad 3 \quad 9 \quad 1$$

$$x^2 \equiv 1, \quad 12 \quad 1.$$

All the roots of the proposed are the residuals of the products of every root of $x^3 \equiv 1$ multiplied by every root of $x^2 \equiv 1$; and its primitive roots, of which there can be only two, and which are evidently 10 and 4, are the residuals of 3×12 and 9×12, the products of the primitive roots of the same equations. The root 12, which belongs to $x^4 \equiv 1$, belongs also to $x^2 \equiv 1$.

PRIMITIVE ROOTS OF PRIME NUMBERS

217. The primitive roots of a prime number p are the primitive roots of the congruence $x^{p-1} \equiv 1$, mod. p; and they have the property that the several powers of any one of them from 1 to $p-1$, when divided by p, leave different remainders. For let α be one of them, then $\alpha, \alpha^2, \alpha^3, \ldots \alpha^{p-1}$ are roots of $x^{p-1} \equiv 1$, and therefore their residuals relative to p are roots; and consequently coincide with $1, 2, 3, \ldots p-1$, which by *Fermat's* theorem are all the roots of $x^{p-1} - 1 \equiv 0$. The primitive roots of any prime number may be found by means of the following propositions.

218. If p be any prime number, and $p - 1 = mn$, then the residuals of the m^{th} powers of $1, 2, 3, \ldots p-1$, relative to p, are roots of the congruence $x^n \equiv 1$, and are therefore in number n and cannot be primitive roots of $x^{p-1} \equiv 1$; and, conversely, if a be any root of $x^n \equiv 1$, then will a be the residual of the m^{th} powers of m of the numbers $1, 2, 3, \ldots p-1$, the congruence $x^m \equiv a$ admitting of m roots.

For let α denote one of the numbers 1, 2, 3, ... $p-1$, and ρ the residual of its m^{th} power so that $\alpha^m \equiv \rho$; then raising both members to the n^{th} power, $\alpha^{mn} \equiv \rho^n$; but by *Fermat's* theorem $\alpha^{mn} = \alpha^{p-1}$ is congruent with 1, therefore ρ^n is congruent with 1, or ρ is a root of $x^n \equiv 1$.

Also if a be a root of $x^n \equiv 1$, then $a^n - 1 = pq$ where q is a whole number; and subtracting each member of this equation from $x^{p-1} - 1$, we get

$$x^{p-1} - a^n = x^{p-1} - 1 - pq.$$

But the first member, which is the same as $x^{mn} - a^n$, has $x^m - a$ for a divisor, therefore the second member admits the same divisor; and consequently (Art. 210) the congruence $x^m \equiv a$ admits of m roots taken from the numbers 1, 2, 3, ... $p-1$; and therefore a is the residual of the m^{th} powers of m of the same numbers.

219. Generally, if p be a prime number, and

$$p - 1 = 2^\rho q^\mu r^\nu \ldots s^\sigma,$$

the non-primitive roots of $x^{p-1} - 1 \equiv 0$, which necessarily belong to one of the congruences

$$x^{\frac{p-1}{2}} \equiv 1,\quad x^{\frac{p-1}{q}} \equiv 1,\quad x^{\frac{p-1}{r}} \equiv 1, \ldots x^{\frac{p-1}{s}} \equiv 1 \ldots\ldots\ldots (1),$$

are, by the preceding proposition, residuals, after dividing by p, of the squares of the numbers 1, 2, 3 ... $(p-1)$; of the q^{th} powers of the same, &c., and of the s^{th} powers of the same. And, conversely, every number that is a residual of the square, of the q^{th} power, &c. or of the s^{th} power, of one of the numbers 1, 2, 3, ... $p-1$, is a root of one of the congruences (1) and cannot therefore be a primitive root of $x^{p-1} - 1 \equiv 0$, or a primitive root of p. We see likewise that half of the numbers 1, 2, 3 ... $p-1$, are the remainders when the squares of the whole of them are divided by p; a q^{th} part of them are the remainders when the q^{th} powers of the whole of them are divided by p; an r^{th} part are the residuals of their r^{th} powers, &c.; and an s^{th} part of the s^{th} powers. And, more generally, if we only consider those amongst the numbers 1, 2, 3 ... $p-1$, which are at once residuals of the squares, q^{th} powers, r^{th} powers, &c., the s^{th} part of these latter will be

at the same time residuals of the s^{th} powers. For the numbers which are at once residuals of the squares, q^{th} powers, r^{th} powers, &c. of the numbers 1, 2, 3, ... $p-1$ satisfy the congruences

$$x^{\frac{p-1}{2}} \equiv 1, \quad x^{\frac{p-1}{q}} \equiv 1, \quad x^{\frac{p-1}{r}} \equiv 1, \text{ \&c.},$$

and consequently are roots of $x^{\frac{p-1}{2qr}} \equiv 1$; their number therefore is $\dfrac{p-1}{2qr\ldots}$. Similarly, the number of those which are at the same time residuals of the s^{th} powers is $\dfrac{p-1}{2qr\ldots s}$, which is the s^{th} part of $\dfrac{p-1}{2qr\ldots}$.

220. To find the primitive roots of a prime number.

Let p be a prime number, 2, q, r, ... s the unequal prime factors of $p-1$: if from the series of numbers

$$1, 2, 3, 4, \ldots p-1, \ldots\ldots\ldots\ldots\ldots (1),$$

we successively remove all those which are residuals of the squares of the above numbers, of the q^{th} powers of the same, of their r^{th} powers, &c., and of their s^{th} powers, when divided by p there will at last remain only primitive roots of p. By means of the residuals of the squares, we exclude half of the numbers (1); by means of the residuals of the q^{th} powers we exclude a q^{th} part of those that remain; and so on, till we arrive at the residuals of the s^{th} powers which are the last to be excluded; and the number of those that finally remain, i. e. the number of primitive roots will therefore be

$$(p-1)\left(1-\frac{1}{2}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots\left(1-\frac{1}{s}\right).$$

Ex. 1. To find the primitive roots of 13.

Here $p-1 = 12 = 2^2 \times 3$; and writing down all the numbers less than 13, and the square of the first half of them, {as the latter half, by reason of the relation $(13-n)^2 \equiv n^2$, must give the same remainders as the first half}, we have

1	2	3	4	5	6	7	8	9	10	11	12, ... (1)
1	4	9	16	25	36,						

and dividing by 13, we get the residuals of the squares

1, 4, 9, 3, 12, 10,

which when removed from (1) leave

2 5 6 7 8 11, ... (2).

The cubes of these, and their residuals after being divided by 13, are

8 125, 216, 343, 512, 1331,

8 8 8 5 5 5.

Suppressing, therefore, the residuals of the cubes from (2), we find 2, 6, 7, 11 for the primitive roots of 13; their number being $12(1-\frac{1}{2})(1-\frac{1}{3}) = 4$.

If we had divided by 13 the cubes of all the numbers (1), we should have found only four different remainders; since all those remainders are roots of $x^4 \equiv 1$.

Ex. 2. To find the primitive roots of 17.

As $17-1=16=2^4$, we have in this case only to reject from the series 1, 2, 3 ... 15, 16, the residuals of the squares of the first half, which are

1, 4, 9, 16, 8, 2, 15, 13;

so that the eight primitive roots of 17 are

3, 5, 6, 7, 10, 11, 12, 14.

For further details on this subject the reader is referred to Serret's *Cours d'Algèbre Supérieure*, from which considerable assistance has been derived.

THE END.

Cambridge Printed at the University Press.

